File 226:TRADEMARKSCAN(R)-US FED OG 030225/AP 030205
(c) 2003 Thomson & Thomson

Set	Items	Description
S1	1	(DESKTOPSTREAMING) OR (DESKTOP()STREAMING)
S2	1	(GOTOMYPC) OR (GO()TO()MY()PC)
S3	0	(EXPERTLIVE) OR (EXPERT()LIVE)
S4	1	CO='EXPERCITY':CO='EXPERCITY.COM, INC.'

?

05709258

DESKTOPSTREAMING

INTL CLASS: 42 (Scientific, technological & legal services)
T&T INTL CLASS: 9 (Electrical & Scientific Apparatus)
U.S. CLASS: 100 (Miscellaneous Service Marks)
101 (Advertising & Business Services)
T&T U.S. CLASS: 21 (Electrical Apparatus, Machines & Supplies)
23 (Cutlery, Machines, & Tools, Parts Therof)
26 (Measuring & Scientific Appliances)
36 (Musical Instruments & Supplies)
38 (Prints & Publications)
STATUS: Registered; Supplemental Register; Intent to Use - Application
GOODS/SERVICES: APPLICATION SERVICE PROVIDER FEATURING AUDIO AND VIDEO STREAMING SOFTWARE FOR TRANSMITTING DATA, GRAPHICS, AUDIO, OR VIDEO OVER ELECTRONIC COMMUNICATIONS NETWORKS
SERIAL NO.: 75-709,258
REG. NO.: 2,679,115
REGISTERED: January 21, 2003
FIRST USE: October 1, 1999 (Intl Class 42)
FIRST COMMERCE: October 1, 1999 (Intl Class 42)
FILED: May 19, 1999
ORIGINAL APPLICANT: JEDIX SOFTWARE SYSTEMS (California Corporation), SUITE 111, 5385 HOLLISTER, SANTA BARBARA, CA (California), 93111, USA (United States of America)
1ST NEW OWNER BEFORE PUBLICATION: EXPERTCITY.COM, INC. (Delaware Corporation), 5385 HOLLISTER, SUITE 111, SANTA BARBARA, CA (California), 93111, USA (United States of America)
ASSIGNEE(S): EXPERTCITY.COM, INC. (Delaware Corporation), 5385 HOLLISTER, SUITE 111, SANTA BARBARA, CA (California), 93111, USA (United States of America)
Assignor(s): JEDIX SOFTWARE SYSTEMS (California Corporation)
Reel/Frame: 2116/0580
Recorded: July 17, 2000
Brief: MERGER
FILING CORRESPONDENT: LARRY COHN , LARRY COHN, STRADLING, YOCCA, CARLSON & RAUTH, 660 NEWPORT CENTER DRIVE, SUITE 1600, NEWPORT BEACH, CA 92660

06219511

GOTOMYPC

INTL CLASS: 9 (Electrical & Scientific Apparatus)
U.S. CLASS: 21 (Electrical Apparatus, Machines & Supplies)
23 (Cutlery, Machines, & Tools, Parts Therof)
26 (Measuring & Scientific Appliances)
36 (Musical Instruments & Supplies)
38 (Prints & Publications)
STATUS: Pending-Published for Opposition; Opposition Filed
GOODS/SERVICES: SOFTWARE FOR USE ON COMPUTERS AND DEVICES FOR ACCESSING, VIEWING, AND CONTROLLING REMOTE COMPUTERS AND DEVICES
SERIAL NO.: 76-219,511
FIRST USE: February 1, 2001 (Intl Class 9)
FIRST COMMERCE: February 1, 2001 (Intl Class 9)
FILED: February 28, 2001
PUBLISHED: June 11, 2002
ORIGINAL APPLICANT: EXPERTCITY.COM (Delaware Corporation), 5385 HOLLISTER AVENUE, SUITE 111, SANTA BARBARA, CA (California), 93111, USA (United States of America)
OWNER AT PUBLICATION: EXPERTCITY.COM (Delaware Corporation), 5385 HOLLISTER AVENUE, SUITE 111, SANTA BARBARA, CA (California), 93111, USA (United States of America)
ASSIGNEE(S): KNOBBE, MARTENS, OLSON & ET AL (Limited partnership) , 2040 MAIN STREET, 14TH FLOOR, IRVINE, CA (California), 92614, USA (United States of America)
Assignor(s): GO2SYSTEMS, INC. (Delaware Corporation)
Reel/Frame: 2576/0060
Recorded: September 16, 2002
Brief: SECURITY INTEREST
OPPOSITION ACTION: 152958
Filed: August 29, 2002
Outcome: PENDING
Date of Outcome: September 24, 2002
Opposing TM: Not Provided
Opposer:
GOTOMYPC.INFO.
;

FILING CORRESPONDENT: CORINE M. FREEMAN , CORINE M. FREEMAN, LYON & LYON, LLP, 633 W 5TH ST STE 4700, LOS ANGELES, CA 90071-2043

DIALOG(R)File 226:TRADEMARKSCAN(R)-US FED

06088347

HELPALERT

INTL CLASS: 9 (Electrical & Scientific Apparatus)
38 (Communications Services)
U.S. CLASS: 21 (Electrical Apparatus, Machines & Supplies)
23 (Cutlery, Machines, & Tools, Parts Therof)
26 (Measuring & Scientific Appliances)
36 (Musical Instruments & Supplies)
38 (Prints & Publications)
100 (Miscellaneous Service Marks)
101 (Advertising & Business Services)
104 (Communications Services)
STATUS: Abandoned - Failure To Respond
GOODS/SERVICES: (INT. CL. 9) SOFTWARE FOR THE PURPOSES OF FACILITATING COMMUNICATIONS IN A GLOBAL COMPUTER NETWORK (INT. CL. 38) SERVICES OF ROUTING ELECTRONIC COMMUNICATIONS
SERIAL NO.: 76-088,347
FIRST USE: January 1999 (Intl Class 9)
January 1999 (Intl Class 38)
FIRST COMMERCE: August 1999 (Intl Class 9)
August 1999 (Intl Class 38)
FILED: July 10, 2000
ABANDONED: November 9, 2001
ORIGINAL APPLICANT: **EXPERCITY**.COM, INC. (Delaware Corporation), 5385 HOLLISTER AVENUE, SUITE 111, SANTA BARBARA, CA (California), 93111, USA (United States of America
FILING CORRESPONDENT: CORRINE M. FREEMAN , CORRINE M. FREEMAN, LYON & LYON, LLP, 633 WEST FIFTH STREET, SUITE 4700, LOS ANGELES, CALIFORNIA 90071-2066

?

Dam
5-4552

GoToMyPC

Log In
Home
How It Works
For You
For Your Company
About Us
Press Highlights
Press Releases
Awards
Contact
Help

"A remarkably useful tool."
BARRON'S

About Us

Expertcity, Inc. was founded in 1997 and has become the leading provider of Web-based remote-access and customer-support technologies. Expertcity's revolutionary remote-access solution, GoToMyPC™, enables both consumers and enterprises to remotely access and work on their PCs from any Internet location. Expertcity Corporate clients include Sun Microsystems, Verizon, Microsoft Business Solutions, Intuit, Kronos, RightNow Technologies, Honeywell, Blackbaud, Cablevision, USDA, Harcourt-Brace, U.S. Department of Trade, Colgate-Palmolive and Fleet Capital.

GoToMyPC Personal is a consumer service that gives individuals unlimited access to heir computers from any Web browser anywhere and enables them to conveniently ınd securely access email, files, programs and network resources from home or the oad. Try GoToMyPC Personal for free.

ɜoToMyPC Corporate is an enterprise version with Web-based administration eatures that allow companies to quickly roll out secure remote-access capability to ıny number of employees. Take a test drive of GoToMyPC Corporate.

ɜet information on DesktopStreaming™, Expertcity's Web-based ASP solution for ustomer support.

Contact | Recommend Us | Become a Partner

b226
S Trac= name
E CO=

GoToMyPC

Log In
Home
How It Works
For You
For Your Company
About Us
Press Highlights
Press Releases
Awards
Contact
Help

"The easiest remote-access tool available."
COMPUTER SHOPPER

Press Releases

May 8, 2002	GoToMyPC Partners with eCommute to Promote Corporate Telework Programs
Apr 1, 2002	Travel Light and Leave Your Laptop at Home
Mar 27, 2002	Expertcity Introduces GoToMyPC Corporate, Making Telework Easy for Businesses
Mar 4, 2002	Insight Services and Expertcity Announce Agreement to Resell GoToMyPC™
Feb 20, 2002	Expertcity Hosts Live Webinar on the Benefits of Web-Based Remote Access for Companies of All Sizes
Feb 4, 2002	GoToMyPC 2.0 Wins Kudos and Awards from Media Giants
Jan 23, 2002	New Telecommuting Technologies Make It Possible to Be Productive While Avoiding Olympic Gridlock
Jan 7, 2002	Americans Seek Ways to Balance Work and Family in 2002
Dec 17, 2001	Expertcity Transfers Its Award-Winning ExpertLive™ Marketplace for Services to Tech24, Inc.
Dec 13, 2001	Technology Helps Workers Be Productive While Battling Winter Workplace Disruptions

Back | Next

GoToMyPC

Log In
Home
How It Works
For You
For Your Company
About Us
Press Highlights
Press Releases
Awards
Contact
Help

Expertcity, Inc. Announces Launch of GoToMyPC.com Public Beta

SANTA BARBARA, CA
February 1, 2001

Expertcity launches public beta of new remote-access application
Expertcity, Inc., a provider of Web-based remote-help technology and services, today announced the launch of its public beta program at GoToMyPC.com™. The new site will be home to GoToMyPC, a Web-based application that allows individuals and enterprises to register their PCs and then access and work on those PCs from any Internet location. Users have full access to all files, programs and network resources available on their desktops. GoToMyPC is firewall friendly and enables easy, highly secure and high-performance remote access to PCs with minimal overhead. GoToMyPC makes working remotely just like being there.

Brian Donahoo, Expertcity's Senior Vice President of Products, says, "GoToMyPC leverages Expertcity's patented DesktopStreaming™ technology to deliver a unique Web-based resource for work extenders, mobile workers and IT managers supporting a distributed workforce."

GoToMyPC's features include:

- Ease of use: Users enjoy full functionality and complete access to all files, programs and network resources on the computer they are accessing. They can use their remote computer as if they were sitting in front of it.
- Secure connection: Uses 128-bit, end-to-end encryption and nested passwords. Because users are authenticated and the computer being accessed is part of a managed domain, this is a more secure solution than a VPN.
- Fast implementation: GoToMyPC is a completely Web-based solution that can be installed companywide in minutes. Companies save money on hardware, software, configuration, user training and support.

GoToMyPC.com's public beta will last from February 1 until April 30, 2001. Enterprises and individuals can simply go to the Web site to register any PC that they wish to make instantly available for remote access and control – no advanced computer skills are required.

\bout Expertcity.com
:xpertcity, Inc. is the leading provider of Web-based remote assistance and :ustomer support solutions. The company was founded in 1999 to introduce its ıroprietary DesktopStreaming technology to the consumer market by offering live ıerson-to-person computer support through a distributed base of certified experts ıt Expertcity.com.

:xpertcity's proprietary DesktopStreaming technology enables customer service epresentatives to chat in real time with their users and quickly escalate to desktop haring, which features mutual mouse and keyboard control and whiteboard apability. The technology supports all major platforms including Windows, Linux, olaris and Mac.

:xpertcity, Inc. has won numerous awards including PC Magazine's Top 100 Sites ınd was recently named a Forbes Best of the Web B2B site. Expertcity, Inc. ıvestors include Sun Microsystems, ZDNet, Bertelsmann Ventures and Wit oundView Ventures. Headquarters are located in Santa Barbara, California.

For media inquiries, contact:
Laura McCormick
Vice President of Corporate Communications
Phone: (805) 690-6435
Fax: (805) 690-6436
Email: laura@expertcity.com

Christie Cooney
Public Relations Specialist
Phone: (805) 690-6448
Fax: (805) 690-6436
Email: christie@expertcity.com

Back

```
?logoff
       27feb03 14:42:32 User258384 Session D1134.2
            $3.73    0.677 DialUnits File226
               $6.60  3 Type(s) in Format  9
            $6.60  3 Types
    $10.33  Estimated cost File226
     $1.16  TELNET
    $11.49  Estimated cost this search
    $11.49  Estimated total session cost   0.833 DialUnits


### Status: Signed Off. (5 minutes)
```

WEST

End of Result Set

Generate Collection Print

L2: Entry 1 of 1 File: USPT Mar 25, 2003

DOCUMENT-IDENTIFIER: US 6538996 B1
TITLE: Remote computer communication

US Patent No. (1):
6538996

Brief Summary Text (3):
Users of remote computers, such as mobile lap-top computers, can often access computers permanently connected to a local corporate network (local computers) using a variety of communication paths. For instance, a user of a remote computer can use a dialed telephone connection to establish a modem-based data link between the remote computer and a remote communication server on the corporate network. Alternatively, the user can use a dialed telephone connection to an access point of a public wide area network, such as the Internet, and then communicate with the corporate network through the wide area network. A user may often have a choice of several different telephone access numbers which he can use to establish a communication path between the remote computer and the corporate network.

Detailed Description Text (3):
As described above, alternative types of communication paths that can be established between remote computer 100 and local computer 110, such as directly, or through the Internet. In addition, alternative paths of each type can be used, for example, using different telephone access numbers or different tunnel servers. Internet 130 and corporate communication system 140 can each have multiple access points to which a telephone connection can be established by dialing particular telephone numbers. For instance, many different companies, called Internet Service Providers (ISPs), each maintain multiple locations that provide telephone access to the Internet 130. These access points are called Points of Presence (POPs). Each POP has a bank of modems that can be accessed by dialing one or more telephone numbers. Alternative points of connection between Internet 130 and corporate communication system 140 can also be available. These connection points can be geographically separated, or can involve use of different communication hardware in corporate communication system 140. A corporation can also provide multiple telephone access points to a corporate network, particularly if it maintains a private geographically distributed network.

Detailed Description Text (13):
First, processor 312 on remote computer 100 communicates with modem 310 in remote computer 100, typically over an internal communication bus or a serial communication line. The modem is configured to be at a particular address, for example, an address associated with a particular communication port index. For example, in the Windows95 operating system, the modem may be configured to be accessible through the second communication port, known as "COM2".

Detailed Description Text (14):
Modem 310 is then connected to PSTN 120, either directly, or through a private switch (private branch exchange, PBX). Modem 310 provides dialing information to PSTN 120 which establishes a telephone connection to a modem 324 at an Internet POP 320. If modem 310 is connected through a PBX, it first provides a dialing prefix or telephone access code to the PBX in order to be connected to PSTN 120.

Detailed Description Text (15):

Modem 324 at Internet POP 320 is coupled to a router 322 at the POP, which provides a gateway to Internet 130. A data path through Internet 130 terminates at a second router 326 that couples Internet 130 and corporate communication system 140.

Detailed Description Text (19):
Establishing the representative communication path shown in FIG. 3 involves several steps. These steps include: Controlling modem 310 from processor 312 in remote computer 100 to connect modem 310 to PSTN 120, get a dial tone, and dial a telephone number for connection to modem 324. Completing a telephone (audio) connection between modem 310 and modem 324. Establishing a raw data connection between modem 310 and modem 324 to provide bidirectional transfer of binary data streams between the modems. Establishing communication between network-layer software executing on remote computer 100 and router 322 at POP 320. This step typically involves an authentication step in which remote computer 100 provides a username and password over the data path established in the previous step. Remote computer 100 can use various communication protocols depending on the capabilities of the POP being accessed. In this instance, the point-to-point protocol (PPP) is used to couple the IP-based network-layer software on remote computer 100 to router 322, thereby allowing the network layer software to send and receive IP-based communication through router 322. Establishing an IP-based communication path between networking software executing on remote computer 100 and tunnel server 332. This requires proper routing of data from networking software on remote computer 110 to router 320, and from router 320 to router 326. Establishing communication between networking software on remote computer 110 and tunnel server software executing on tunnel server 332. In this instance, an enhanced tunnel protocol, which includes features of the Point to Point Tunnel Protocol (PPTP), is used. Alternatively, protocols such as L2TP and IPsec can be used to provide tunneling capabilities. This step involves authenticating the remote user. Once remote computer 100 is connected to tunnel server 332 and the remote user authenticated, the tunnel server software provides a service to networking software on remote computer 100 so that remote computer 100 can communicate on LAN 340 as if it were directly connected, using a variety of communication protocols, such as IP, IPX, and NetBUI. This type of connection is termed a "virtual private network" (VPN) because remote computer 100 is virtually on LAN 340.

Detailed Description Text (21):
Other types of communication paths follow similar routes. A connection path through direct Internet access network 125 (FIG. 1) is similar to the path shown in FIG. 3. For instance, if direct Internet access network 125 is a CATV network, modems 310 and 324 are replaced with CATV modems, and PSTN 120 is replaced with the CATV network. The steps involved are also similar, except that a dialing step is not required because the cable modems are connected to each other when they power on.

Detailed Description Text (22):
Referring to FIG. 4, remote computer 100 can communicate without using Internet 130 (depicted in FIG. 3). In this case, a dialed telephone connection terminates at a modem 412 at a remote access server 410. Remote access server 410 communicates directly with LAN 340. Communication between networking software executing on remote computer 100 and remote access software executing on remote access server 410 can use a variety of communication protocols depending on the capabilities of remote access sever 410. In this instance the remote access software uses PPP.

Detailed Description Text (24):
Referring to FIG. 5, connection software executing at remote computer 100 (FIG. 1) includes several cooperating modules. At a low level, a modem includes modem firmware 548 that executes on a controller that is part of the modem hardware and implements various data communication protocols, and an NDIS interface 549 provides an interface to direct access network 125. Modem firmware 548 implements communication functions, including a capability to negotiate use of a compatible protocol with another modem to which it connects.

Detailed Description Text (25):
Communication services 535, applications 590 and other software modules interface with communication drivers 540. Communication drivers 540 include communication port drivers 542 execute on main processor 312 of remote computer 100 and provide a

low-level interface to the modem firmware 548. An NDIS driver 543 provides a low-level interface to NDIS driver 549. A tunnel driver 544 provides both provides driver-level services to communication services 535, and makes use of communication service 535 to implement tunneled communication between remote computer 100 and tunnel server 332. Communication services 535 includes a transport layer module, TCP 536, and network layer module, IP 537, and a data link module, PPP 538. Tunnel driver 544 implements the enhanced tunnel protocol, ATN. Remote access services/dialup networking (RAS/DUN) module 530 controls the establishment of remote connections, making use of communication services 535. Once a remote connection is established, communication services 535 provide services directly to applications 590.

Detailed Description Text (29):
A modem interface 544 provides low-level modem-based communication services to prescriber 560 and access 550. For example, in the event that RAS/DUN 530 is unable to establish a connection through communication services 535, prescriber 560 can attempt to diagnose the difficulty by accessing the modems through modem interface 544. Call home 546 also uses modem interface 544 to establish a communication path between remote computer 100 and management server 334. Access 550 and prescriber 560 can use file transfer 547, which in turn uses call home 546 to obtain data from management server 334 prior to establishing a network-based connection.

Detailed Description Text (44):
Referring to the flowchart in FIG. 11, when automation server 510 provides the connection path list to connect library 520 (step 850 in FIG. 8), connect library 520 performs the series of steps shown. After connect library 520 accepts the connection path list (step 1100), it first determines whether remote computer 100 already has an IP connection to Internet 130 (step 1110). For example, the user may have previously made a telephone connection to a POP, or the remote computer may have an IP connection through a CATV modem.

Detailed Description Text (68):
We turn now to situations in which connect library 520 is unsuccessful in establishing a connection to a POP or to a tunnel server (steps 1126 and 1146 in FIG. 11). When connect library is unsuccessful in establishing a connection, it calls prescriber 560 (step 1160 in FIG. 11) to attempt to resolve the problem. Referring to FIG. 17, prescriber 560 includes three components. A prescriber control 1710 accepts error information from connect library 520 and initiates handling of those errors. In response to prescriber control 1710, an interpreter 1720 processes scripts 562 written in the "tcl" (Tool Command Language) scripting language. These scripts invoke procedures in interface routines 1730 which provide a mechanism for interacting with other modules of the connection software, including call home 546, modem interface 544, and RAS/DUN 530.

Detailed Description Text (71):
Top-level scripts 1740 first classify an error into one of a number of types based on the error message. The first type of error relates to RAS/DUN 530 not being able to establish a connection, but not encountering any hardware or software errors. A condition that might cause this type of error is a POP simply not answering the telephone. A second type of error relates to hardware errors, such as a modem malfunctioning. A third type of error relates to software errors. Such an error may be caused, for example, by improper installation of a device driver. A fourth type of error relates to unsuccessful authentication or initiation of a communication protocol. Another type of error relates to errors encountered by connect library 520 itself, such as not being able to call RAS/DUN 530. Depending on the type of error message received, top-level script 1740 branches to a particular secondary script 1750 to further address the problem.

Detailed Description Text (73):
If the error message passed from connect library 520 to prescriber 560 indicates that a telephone connection could not be established, but that there is no hardware or software error, prescriber 560 attempts to make a telephone connection itself. First, it determines that it indeed is able to obtain a dial tone by controlling the modem directly using routines in modem interface 544. If a dialtone is detected and a dialing prefix (e.g., "9") is needed to access PSTN 120, prescriber 560 dials the

prefix and confirms that it again obtains a dial tone. If a dial tone is not obtained, the prescriber attempts to dial the telephone access code without dialing the prefix in case the dialing prefix was not in fact needed. If prescriber 560 cannot connect without a prefix, and cannot obtain a dial tone with the specified prefix, it tries several alternatives based on the calling location (e.g., typical prefixes for the country the user is calling from), and, after exhausting normal alternatives, it prompts the user to enter new prefix information. If no dialtone can be obtained, prescriber 560 prompts the user to confirm that the modem is properly connected to the telephone line. If prescriber 560 can obtain a ring, but the call to the access number is not answered, it returns to connect library 520 with the response that the connect library should attempt to use the next connection path, which is associated with a different telephone number. If prescriber 560 completes a call to the access number but is unable to establish a data connection, it next tries to rule out problems with the modem itself. As the called modem may be at fault rather than modem 310 at the remote computer, prescriber 560 calls a reference modem that is known to function. In particular, a special reference modem 335 (FIG. 3) is attached to management server 334. Prescriber 560 obtains the telephone number for this reference modem from access 550 and dials the connection. If the modem 310 is not able to establish a data connection with the reference modem 335, the configuration of modem 310 is suspect. One source of problem the modem may have is in attempting to negotiate a modem protocol with the called modem. Prescriber 560 attempts to call reference modem 335 again, this time using a specific modem protocol. In particular, the modem protocol used is the most basic protocol that has the greatest chance of actually connecting. If this too fails, then the modem hardware is likely at fault.

Detailed Description Text (74):
If the error message indicates a hardware error, prescriber 560 performs some of the same steps to determine the cause of the hardware error. Using modem interface 544, it first verifies that it can actually establish communication with the modem. For instance, many modems provide a command monitor in firmware which executes on the modem and which processes commands and status inquiries. If prescriber 560 determines that it is indeed able to interact with the command monitor without a hardware error, it attempts to make a telephone connection to the access number. It can again attempt to go through the steps to establish communication with the current access number in the connection path list, and can also call the reference modem 335 at the management server.

Detailed Description Text (75):
Even though a connection to a POP cannot be established, prescriber 560 may successfully connect to management server 334. If such a connection is possible, prescriber 560 can establish a connection through call home 546 to call home 760 on management server 334. In certain cases, a modem hardware problem may be correctable by upgrading the modem firmware. Call home 760 uses access 712 to determine whether any appropriate firmware updates are available. If one is available that may be relevant, it is transferred to prescriber 560 which then performs the steps necessary to install the new firmware.

Detailed Description Text (76):
If prescriber 560 is able to connect to the reference modem using a specific modem protocol, such as a slow speed protocol that does not use features such as error correction or encryption, the prescriber can instruct connect library 520 to attempt to connect to the current POP using that same protocol. In this way, a remote user may establish a connection path, although the path may be slower than desired.

Detailed Description Text (77):
In the case of a software error, two common problems addresses by prescriber 560 are software misconfiguration and software version mismatch. To determine whether modem 310 is accessible through comm driver 542, prescriber 560 attempts to access the modem. To determine which port the modem is connected to, prescriber 560 reads registry 580. Registry 580 includes information written by RAS/DUN 530 that allows prescriber 560 to determine which port was used on the last dialing attempt by RAS/DUTN 560. Once prescriber 560 determines which port was used, it attempts to communicate with the modem on that port through modem interface 544. Modem interface 544 provides high level routines that are used to access and configure modem 310.

Detailed Description Text (78):
If modem 310 is not accessible through comm driver 542, prescriber 560 checks whether the comm driver appears to be functioning properly by accessing various routines provided by the driver. If the driver does not seem to be functional, prescriber 560 reinstalls the driver if it has a copy on a local disk on remote computer 100. If prescriber 560 determines that the driver needs to be reinstalled, and doesn't have a local copy, it obtains a copy from management server 344 using call home 546. Call home 546 places a telephone call and communicates with a modem at the managements server. A corresponding call home module on the management server provides the required driver by transferring a file over the modem connection using a low level file transfer protocol, in this instance, using the ZMODEM protocol. Prescriber 560 reinstalls the driver, and causes the operating system to reboot itself in order to complete the installation process. In order to maintain its state through the reboot, prescriber 560 writes information in access 550 before rebooting the system.

Detailed Description Text (80):
To determine whether a connection between modem 310 and the modem at the POP can be established, prescriber 560 can dial the POP directly using modem interface 544. If a modem connection is established, then prescriber 560 can assume the problem was encountered during the process of providing login information, or in establishing the communication protocol, such as PPP, that was to be used to communicate between the remote computer and the POP.

Detailed Description Text (82):
Prescriber 560 maintains a diagnostic log 1760 (FIG. 17) which records its activities. When a connection to management server is established, this information is passed through delivery 572 and delivery 710 to logging service provider 740 (FIG. 7) which collects information from various remote computers in a log 742. This log can be used to discover consistent problems encountered by more than one remote computer. For example, a particular telephone access number may not function correctly. This information can be used to update the information used by access 550 in determining connection path lists so that calls to the non-functional access number are not attempted. In addition to automatically scanning log 742 to modify master client database 722, errors encountered by prescriber 560 can be used to automatically generate "trouble tickets" in an associated help desk system. In addition, failed attempts to connect to a reference modem on the management server, or failed attempts to connect to tunnel server 332 can be matched to logged events at the remote computer, and associated with a single trouble ticket.

Detailed Description Text (84):
Prescriber scripts 562 are downloadable from management server 334. These scripts are provided to management server 334 from a centralized site along with or as part of distribution database 772. In this way, as new approaches to diagnosing problems on remote computers are developed, they are available to remote computers 100. Along with updated scripts, software updates, such as drivers and modem firmware, can also be distributed from the central location. The connection system can therefore support many more diagnostic strategies than those described above, as those strategies are implemented in scripts that can be downloaded at a later date.

Detailed Description Text (86):
Prescriber scripts make use of extensions to the tcl language, in the form of built-in functions, that are used to interact with other software modules on the remote computer. A function is provided to determine the serial (COMM) port corresponding the a RAS entries. Functions are provided to open, close, write to, and read from, a modem attached to a specified serial port. A function is provided to initiate a reboot process. This function stores information in non-volatile memory that is used by the prescriber after the reboot is complete to determine that it itself initiated the reboot process, and that it should invoke the top level reboot script. A function is also provided to communicate with access 550 to access local database 552 or data stored on the management server. Another function is used to communicate with call home 546 and file transfer 547. This function includes the option of communicating with a reference modem at the management server to verify the proper functioning of the local modem, as well as the option to retrieve files

or configuration parameters from the management server.

CLAIMS:

28. A diagnostic script stored on a computer readable medium including instructions that cause a computer to diagnose and correct a problem encountered while attempting to communicate with a computing resource remote from the computer, including instructions for contacting a reference site remote from the computer and verifying that the computer can communicate with the reference site wherein diagnosing and correcting the problem includes invoking a procedure to verify proper operation of a local modem on the computer, including establishing a telephone connection to a remote modem and transferring data between the local modem and the remote modem.

L8: Entry 2 of 6 File: USPT Mar 25, 2003

DOCUMENT-IDENTIFIER: US 6538996 B1
TITLE: Remote computer communication

Brief Summary Text (3):
Users of remote computers, such as mobile lap-top computers, can often access computers permanently connected to a local corporate network (local computers) using a variety of communication paths. For instance, a user of a remote computer can use a dialed telephone connection to establish a modem-based data link between the remote computer and a remote communication server on the corporate network. Alternatively, the user can use a dialed telephone connection to an access point of a public wide area network, such as the Internet, and then communicate with the corporate network through the wide area network. A user may often have a choice of several different telephone access numbers which he can use to establish a communication path between the remote computer and the corporate network.

Brief Summary Text (6):
Having chosen a desired access telephone number, the user may not be successful in establishing a data communication channel using that telephone number. Establishing a communication channel requires proper operation and interaction of a large number of software and hardware elements. A hardware or software failure, misconfiguration, or incompatibility, in one or more elements in the communication path can prevent a connection from being successfully established. Failures can also occur at any of a number of steps which must be carried out to establish a communication channel. These include failure to properly connect to a telephone line, improper dialing due to an incorrect telephone number or incorrect dialing prefix, unsuccessful connection to an ISP due to hardware or software problems at the POP, unsuccessful or poor data transfer over the Internet, unsuccessful connection to a tunnel server, unsuccessful communication between the remote computer and software executing on the tunnel server, and unsuccessful communication between a tunnel server and other computers on the LAN.

Brief Summary Text (9):
Another aspect of remote communication that often introduces complexity, and may be a source of errors, relates to security. In order to control access to wide area and local area networks, and access to particular computers or systems accessible over those networks, a user must typically interact with multiple authentication and authorization systems. It is not uncommon for a remote user to have to supply one password when connecting to a wide area network, another to establish a connection to a corporate network, and yet another when finally accessing a computer system, such as a mail server.

Brief Summary Text (11):
In one aspect, in general, the invention provides software, stored on a computer readable medium, for causing a remote computer to establish a data communication path to a computing resource, such as a data network. The method includes determining a set of access paths for communicating between the remote computer and the computing resource, and evaluating a cost function which characterizes the cost of communicating between the remote computer and the computing resource over that access path. The cost function can includes both monetary and performance related factors. The method also includes selecting a best one of the access paths according to the evaluated cost functions for the access paths, for example selecting the lowest cost path, and then initiating establishment of communication over the

selected best access path. The access path can feature a dialed telephone channel to a telephone access number associated with that access path, and establishment of communication over the access path can include dialing the telephone access number.

Brief Summary Text (12):
The method can also feature accepting an identification of a location of the remote computer determining a set of access paths according to the telephone charges associated with use of dialed telephone channels to each of the telephone access numbers from the location of the remote computer.

Brief Summary Text (14):
The method can also feature the remote computer accepting a dialing database which includes telephone access numbers, and accepting an identification of the computing resource with which a communication channel is to be established. The remote computer then accesses the dialing database to determine the set of access paths for communicating with the computing resource.

Brief Summary Text (17):
In anther aspect of the invention, in general, the invention provides software for causing a computer, such as a management server, to store a dialing database, including telephone access numbers for access paths, and establish an authenticated management communication path between the computer and a remote computer. The computer then provides information from the dialing database to a remote computer, for use on the remote computer in selecting an access path between the remote computer and a computing resource.

Brief Summary Text (18):
The execution of the software can also feature accepting master dialing information and accepting local information, including information related to computing resources accessible from the remote computer, and maintaining the dialing database using the master dialing information and the local information. The master dialing information can include telephone access numbers for access paths, and information related to a cost of communicating over dialed telephone connections to those access numbers from remote locations.

Drawing Description Text (4):
FIG. 3 is an exemplary connection path joining a remote computer and a local computer through a telephone network, an Internet, and a LAN;

Drawing Description Text (10):
FIG. 9 is a flowchart of a procedure used by an access module on a remote computer to assemble a list of connection paths;

Drawing Description Text (11):
FIG. 10 shows data structures of a connection path list assembled by an access module on a remote computer;

Drawing Description Text (13):
FIG. 12 shows data structures used by an access module on a remote computer to assemble a list of connection paths;

Detailed Description Text (2):
Referring to FIG. 1, an illustrative embodiment of the invention features one of a number of remote computers 100 communicating with one or more local computers 110 that are coupled directly to a corporate communication system 140. Corporate communication system 140 is made up, for example, of a local area network (LAN) and communication related computers and routing devices coupled to the network. Remote computer 100 can establish a variety of communication paths to a local computer 110, three examples of which are shown in FIG. 1. For example, remote computer 100 can use public switched telephone network (PSTN) 120 to establish a dialed telephone connection coupling remote computer 100 directly to corporate communication system 140. Alternatively, remote computer 100 can establish a dialed telephone connection to couple the remote computer to Internet 130. In this case, a communication path through Internet 130 then completes a connection path from remote computer 100 to corporate communication system 140, to which local computer 110 is coupled. Remote

computer 100 can also be coupled to a direct Internet access network 125. Direct Internet access network 125 can use a variety of communication approaches, such as a cable television (CATV) network, a digital subscriber loop (xDSL) data connection over local telephone wiring, or a cellular digital packet data (CDPD) wireless connection. A communication path from remote computer 100 through direct Internet access network 125, Internet 130, and corporate communication system 140 then couples remote computer 100 and local computer 110.

Detailed Description Text (3):
As described above, alternative types of communication paths that can be established between remote computer 100 and local computer 110, such as directly, or through the Internet. In addition, alternative paths of each type can be used, for example, using different telephone access numbers or different tunnel servers. Internet 130 and corporate communication system 140 can each have multiple access points to which a telephone connection can be established by dialing particular telephone numbers. For instance, many different companies, called Internet Service Providers (ISPs), each maintain multiple locations that provide telephone access to the Internet 130. These access points are called Points of Presence (POPs). Each POP has a bank of modems that can be accessed by dialing one or more telephone numbers. Alternative points of connection between Internet 130 and corporate communication system 140 can also be available. These connection points can be geographically separated, or can involve use of different communication hardware in corporate communication system 140. A corporation can also provide multiple telephone access points to a corporate network, particularly if it maintains a private geographically distributed network.

Detailed Description Text (6):
Referring to FIGS. 2(a-c), after a remote user initiates execution of a connection software system on remote computer 100, the user provides information to two, and possibly three interactive dialog boxes. In a first dialog box 210, shown in FIG. 2(a), the user provides a username 212 and a password 214. After the system accepts the information provided in dialog box 210, the user is presented with a second dialog box 220, shown in FIG. 2(b). The user provides information related to the location from which the user is calling 222 and information related to the point to which the user wants to connect 224. The "calling from" information 222 is typically a telephone number, including at least an area code, also known as a number plan area (NPA), and a telephone exchange within that area code. Rather than specifying a telephone number, the user can choose from a "pull-down" list of names associated with telephone numbers stored in the remote computer. The "calling from" entry can also be an indication that the remote computer is already connected to the Internet. The "calling to" information 224 is an identifier of a particular access point within corporate communication system 140 to which the user wants to be connected. For example, in a geographically distributed corporate communication system, the user may specify the particular location to which the user wants to be connected. Access points can be associated with an Internet address or a telephone number of a server computer coupled to corporate communication system 140. The "calling from" field 222 and the "calling to" field can each present a set of choices from which the user may select one, or the user can enter another value that is not in the set of presented choices. The choices are in part preconfigured into the system by an administrator of the system, and can also include recently used field values. For example, if a user is staying at a particular remote location for some time, the user may repeatedly use the same "calling from" telephone number. The "calling from" field also accepts other information related to the location of the remote location, such as dialing prefixes that are required to establish a telephone connection, and telephone services (such as call waiting) that should be disabled before establishing a data connection on the telephone line. Alternative user interfaces can also be used. For example, the dialog boxes shown in FIGS. 2(a) and 2(b) can be combined into one.

Detailed Description Text (8):
Alternatively, the user can press (e.g., activating using a mouse) a "more" button 228 to view information related to the connection that would be established if the user were to connect at that point. In response, as indicated in FIG. 2(c), possible communication paths identified by the connection software to couple remote computer 100 and the selected access point within corporate communication system 140 are presented in a list of connection paths 232. The list is sorted so that the first

entry in the list is the path preferred by the connection software. Preference is based on a calculated cost for each of the paths, including both monetary and performance related factors. Each entry in the list includes path information, such as the ISP that would provide access to the Internet and communication characteristics, such as data rate. Depending on the configuration of the system, the list may include an indication of the cost of using that connection, and a user may be given the right to reorder the list, or to otherwise indicate that a path that is not the lowest cost path is his preferred choice. Having viewed, and possibly modified the order of connection paths 232, the user initiates the connection procedure by activating "connect" button 226.

Detailed Description Text (12):
Establishing a connection path between remote computer 100 and local computer 110 can involve several steps associated with establishing different segments of the path. FIG. 3 shows a representative communication path such as might be established between remote computer 100 and local computer 110. The path uses a dialed telephone connection from remote computer 100 to an Internet POP 320 and an Internet-based connection from POP 320 to local computer 110. The communication path includes several physical segments.

Detailed Description Text (14):
Modem 310 is then connected to PSTN 120, either directly, or through a private switch (private branch exchange, PBX). Modem 310 provides dialing information to PSTN 120 which establishes a telephone connection to a modem 324 at an Internet POP 320. If modem 310 is connected through a PBX, it first provides a dialing prefix or telephone access code to the PBX in order to be connected to PSTN 120.

Detailed Description Text (15):
Modem 324 at Internet POP 320 is coupled to a router 322 at the POP, which provides a gateway to Internet 130. A data path through Internet 130 terminates at a second router 326 that couples Internet 130 and corporate communication system 140.

Detailed Description Text (16):
Corporate communication system 140 includes a local area network (LAN) 340. A firewall 330 is coupled to LAN 340. Firewall 330 is connected to router 326, for example over a high-capacity leased telephone line, and provides a gateway between Internet 130 and corporate communication system 140. Also on LAN 340 is a tunnel server 332 and a management server 334.

Detailed Description Text (19):
Establishing the representative communication path shown in FIG. 3 involves several steps. These steps include: Controlling modem 310 from processor 312 in remote computer 100 to connect modem 310 to PSTN 120, get a dial tone, and dial a telephone number for connection to modem 324. Completing a telephone (audio) connection between modem 310 and modem 324. Establishing a raw data connection between modem 310 and modem 324 to provide bidirectional transfer of binary data streams between the modems. Establishing communication between network-layer software executing on remote computer 100 and router 322 at POP 320. This step typically involves an authentication step in which remote computer 100 provides a username and password over the data path established in the previous step. Remote computer 100 can use various communication protocols depending on the capabilities of the POP being accessed. In this instance, the point-to-point protocol (PPP) is used to couple the IP-based network-layer software on remote computer 100 to router 322, thereby allowing the network layer software to send and receive IP-based communication through router 322. Establishing an IP-based communication path between networking software executing on remote computer 100 and tunnel server 332. This requires proper routing of data from networking software on remote computer 110 to router 320, and from router 320 to router 326. Establishing communication between networking software on remote computer 110 and tunnel server software executing on tunnel server 332. In this instance, an enhanced tunnel protocol, which includes features of the Point to Point Tunnel Protocol (PPTP), is used. Alternatively, protocols such as L2TP and IPsec can be used to provide tunneling capabilities. This step involves authenticating the remote user. Once remote computer 100 is connected to tunnel server 332 and the remote user authenticated, the tunnel server software provides a service to networking software on remote computer 100 so that remote

computer 100 can communicate on LAN 340 as if it were directly connected, using a variety of communication protocols, such as IP, IPX, and NetBUI. This type of connection is termed a "virtual private network" (VPN) because remote computer 100 is virtually on LAN 340.

Detailed Description Text (21):
Other types of communication paths follow similar routes. A connection path through direct Internet access network 125 (FIG. 1) is similar to the path shown in FIG. 3. For instance, if direct Internet access network 125 is a CATV network, modems 310 and 324 are replaced with CATV modems, and PSTN 120 is replaced with the CATV network. The steps involved are also similar, except that a dialing step is not required because the cable modems are connected to each other when they power on.

Detailed Description Text (22):
Referring to FIG. 4, remote computer 100 can communicate without using Internet 130 (depicted in FIG. 3). In this case, a dialed telephone connection terminates at a modem 412 at a remote access server 410. Remote access server 410 communicates directly with LAN 340. Communication between networking software executing on remote computer 100 and remote access software executing on remote access server 410 can use a variety of communication protocols depending on the capabilities of remote access sever 410. In this instance the remote access software uses PPP.

Detailed Description Text (23):
Other types of paths can also be supported but are not illustrated. For instance, a direct telephone connection between remote computer 100 and remote access server 410 can be used, whereby communication passes through tunnel server 332 before reaching local computer 110. Tunnel server can provide encryption or compression services that may not be available when using remote access server 410 alone.

Detailed Description Text (27):
The previously mentioned software modules access 550, authorization 570, and delivery 572, provide services to other software modules of the connection software. Access 550, in addition to computing the list of connection paths requested by automation server 510 and used by connect library 520, provides an interface to a distributed database. The distributed database has data stored both in a local database 552 as well as on management server 334. This database includes a variety of information, including user preferences. Authorization 570 provides authorization related services to other software modules. For example, authorization 570 accepts the username and password provided by the user, and provides those and related credentials to other modules that require them during the process of establishing and maintaining a communication path. Delivery 572 provides communication services between software modules executing on remote computer 100 and services that allow software modules executing on remote computer 100 to communicate with software modules executing on other computers, such as tunnel server 332 and management server 334. For instance, delivery 572 accepts logging information from other modules on remote computer 100 and sends that information to a centralized logging service provider executing on management server 334. Delivery 572 enforces a ring-based security mechanism (described below), and provides addressing and routing services for various modules. Delivery makes use of communication services 535 to communicate with other computers.

Detailed Description Text (32):
When remote computer 100 communicates with management server 334 through tunnel server 332, that communication passes through tunnel protocol 600. Other communication, such as communication from local computer 110 to remote computer 100 also passes through tunnel protocol 600. Tunnel protocol 600 provides a prioritization service. In particular, management server 334 provides data for access 550 on remote computer 100 in order that access 550 can keep local database 552 up to date. This update information is requested by access 550 and is sent as a background activity, in a manner that minimizes the impact on other communication between remote computer 100 and, for example, local computer 110. Data sent from management server 334 to tunnel server 332 can be tagged as having a lower priority than other communication destined for remote computer 100. Tunnel protocol 600 implements sends higher priority messages to remote computer 100 in preference to messages tagged with a lower priority. In this way, transfer of information to

update local database 552 does not appear to impact communication between applications 590 and, for example, local computer 110.

Detailed Description Text (34):
Service providers that execute on management server 334 include an access service provider 720. Access service provider 720 accesses a master client database 722 and corporate database 774. Access modules, such as access 712, access 622 on tunnel server 332, or access 550 on remote computer 100, communicate with access service provider 720 in order to retrieve data in master client database 722 and to store and retrieve data in corporate database 774. Master client database 722 includes data needed to select a lowest cost connection path from a remote computer 100.

Detailed Description Text (36):
A logging service provider 740 provides a centralized mechanism for tracking behavior of various software modules on computers, such as on one or more remote computers 100. This logged information is stored in a log 742. A monitor 743 can process the information in log 742 and use this information to update corporate database 774. For example, if a particular access path has repeatedly been inaccessible to remote computers, the telephone access number for that path may be given a very high cost so that remote computers avoid needlessly trying to connect through that access number.

Detailed Description Text (38):
Master client database 722 includes information needed to select a lowest-cost connection path from a remote computer 100 to corporate communication system 140. This information is configured by database maintenance 770 using a distribution database 772, which does not necessarily contain information specific to the particular corporation, and a corporate database 774 which contains information that is specific to that corporation. Specific information includes assignment of users to particular user groups, connection policy information for those user groups, and connection information such as telephone access numbers for remote communication servers or POPs not included in distribution database 772. Distribution database 772 is obtained by database distribution 776, for instance by a file transfer from a centralized server on the Internet. Alternatively, distribution database 772 may be provided by distribution of physical media, such as CD-ROMs.

Detailed Description Text (39):
In operation, software modules on a remote computer 100, on a management server 334, and on a tunnel server 332 cooperate to establish a connection path between remote computer 100 through tunnel server 332 to a local computer 110. Software modules communicate through a management communication channel maintained by the delivery service modules on the various computers involved in a connection. This management communication channel provides a secure means of coordinating the distributed software modules.

Detailed Description Text (44):
Referring to the flowchart in FIG. 11, when automation server 510 provides the connection path list to connect library 520 (step 850 in FIG. 8), connect library 520 performs the series of steps shown. After connect library 520 accepts the connection path list (step 1100), it first determines whether remote computer 100 already has an IP connection to Internet 130 (step 1110). For example, the user may have previously made a telephone connection to a POP, or the remote computer may have an IP connection through a CATV modem.

Detailed Description Text (45):
If the remote computer does not already have an IP connection to the Internet, connect library 520 initiates a dialup procedure to the telephone number of the first POP in pop list 1010 of connection path list 1000 (FIG. 10) (step 1120). Connect library 520 initiates this dialup procedure by creating a temporary connection record indicating the POP number, and the credentials needed to establish a connection to that POP, and storing this record on disk. Connect library then requests from RAS/DUN 530 that it attempt to establish a connection using the stored temporary connection record.

Detailed Description Text (46):

RAS/DUN 530 is a component of the Microsoft Windows95 operating system. Direct user interaction by RAS/DUN 530 is inhibited, or at least hidden from the user. Connect library 520 controls RAS/DUN 530 and instructs it to use the temporary connect record it has just written to disk. RAS/DUN 530 attempts to make the telephone connection, as well as the network connection, using the specified protocol, such as PPP. RAS/DUN 530 uses the credentials stored in the temporary connect record to establish the network connection that provides access to the Internet through the POP identified in the temporary connect record.

Detailed Description Text (47):
If the connection to the Internet through the first POP succeeds (step 1126), that is, RAS/DUN 530 returns a successful status message, connect library 520 next determines whether a tunnel connection is needed (step 1130) by checking whether tunnel list 1020 (FIG. 10) includes any entries. If a tunnel connection is required, connect library 520 creates a second temporary connection record indicating the desired tunnel server and credentials needed to connect, and requests from RAS/DUN 530 that it attempt to establish a connection using the second temporary connection record. If a tunnel connection is not required (step 1130) or if a tunnel connection is successfully established (step 1146), connect library 520 provides automation server 510 with a notification of the successful connection (step 1150).

Detailed Description Text (54):
The monetary and performance factors stored in records of ISP table 1240 and POP table 1230 are numbers that represent a level for each factor. Examples of monetary factors include the charge to initiate a connection through an ISP, and a per hour usage charge. A record of ISP table 1240 can also include information related to a threshold cumulative connection time beyond which a monetary factor is applied. This is used, for example, in the case that an ISP provides a number of includes connection hours each month, beyond which an hourly connection charge applies. Local database 552 is used to store the accumulated time in each period that is used to determine whether the threshold has been exceeded. Examples of performance factors include a speed factor which is a higher number for slow data rate connections, a delay factor which is a high number for connections that suffer high latency in delivery of packets, and an error factor which is high if a large number of data packets are lost in transmission. In other words, the monetary and performance factors enable one to computer a relative cost associated with using a particular POP. Note that both the POP and the ISP can have performance factors associated with them. For example, a POP's error factor may be the result of poor telephone service to the POP resulting in corrupted data transmissions between a remote computer and a POP, while an ISP may have a high error factor due to use of an overloaded backbone in the Internet resulting in packets being dropped at intermediate nodes in that backbone network. Also, monetary factors may depend on a POP. For instance, a POP accessed through a toll-free telephone number may have a surcharge over another POP operated by that ISP which is accessed by non-toll-free telephone calls.

Detailed Description Text (56):
Local database 552 also includes information that provides the Internet hostname or IP address of tunnel servers used to connect to particular destinations. The "calling to" field provided by the user is used to determine whether a tunnel server is needed, and, if one is needed, the one or more tunnel servers that can provide access to the "calling to" destination. Associated with each tunnel server is access information including information used to determine the type of tunnel connection that should be established, such as the tunnel protocol, and various encryption and compression options.

Detailed Description Text (57):
NPA tables 1200, POP table 1230, and ISP table 1240, together termed the dialing tables, are computed at management server 334 and transferred to remote computer 100 at the request of access 550. The process of creation of these tables is shown in FIG. 13. This process is performed on a multiple computers as is described below.

Detailed Description Text (58):
Referring to FIG. 13, the first stage in computing the dialing tables uses a telephone rate database 1310 and a POP information database 1312. This stage is performed at a centralized location, serving many different corporations, such as a

centralized server computer on the Internet 130. Also incorporated into distribution database 1330 is information from software and scripts 1314 that can include prescriber scripts and software updates for modules on remote computers. This database assembly stage does not incorporate corporation specific information. Telephone rate database 1310 is a database, such as one provided by the Center for Communication Management Information (CMMI) which includes sufficient information for telephone companies to price domestic telephone calls in the U.S. and Canada based the source and destination telephone numbers. One aspect of this information relates to definition of local calling areas. A local calling area for a source telephone number defines the destination telephone numbers for which no toll charges are applied by a telephone company handling the call. The structure of the data provided in telephone rate database 1310 is described in more detail below. POP information database 1312 includes information related to ISPs and the POPs that they operate. In particular, for each ISP, telephone access numbers the POPs operated by that ISP are listed. In addition, data rate and pricing information associated with each telephone access number is also included.

Detailed Description Text (59):
Distribution database assembly 1320, a software process that executes on a centralized server computer, takes local calling information from telephone rate database 1310, and information in POP information 1310 and creates a set of relational database tables, the format of which is described below. These tables are transferred to management server 334 over the Internet and accepted by database distribution 776 (FIG. 7) executing on the management server. Database distribution 772 creates a local copy of distribution database 772 which is stored on management server 334.

Detailed Description Text (62):
In response to a request from access 550 (FIG. 5) executing on remote computer 100, access service provider 720 sends relevant portions of master client database 722 or corporate database 774 to the remote computer. Access 550 stores those received portions in local database 552 on remote computer 100. Access 550 requests data in order of potential importance to a user to remote computer 100. For example, dialing information for the current location the remote computer is calling from is more important than information for other locations. Locations that have been visited recently are more important than locations that are rarely visited. In this way, although the whole master client database may not be updated, the parts most likely to the useful to a user are requested. Also, if a connection is terminated while data is being transferred to access 550, the transfer is restarted the next time a connection is established.

Detailed Description Text (81):
If connect error occurs while attempting to establish communication with tunnel server 332, prescriber 560 first checks whether it can communicate with other well known addresses on the Internet. It can attempt to communicate with a well known domain name server (DNS). Also, it can attempt to communicate with router 326 that provides connectivity between corporate communication network 140 and Internet 130. Finally it attempts to communicate with tunnel server 332. Depending on which of these Internet addresses are accessible from remote computer 100, prescriber may take different courses of action. For example, if router 326 is accessible, but tunnel server 332 is not, it can return to connect library 520 with instructions to try to connect to the next tunnel server in the connection path list. If on the other hand router 326 is not accessible, the problem may be with the ISP's backbone, which may not provide connectivity to router 326 or may be experiencing a high error rate preventing a connection from being established. In such a case, prescriber 560 can return instructions to connect library 520 to go back and establish a POP connection to the next POP in the connection path list. In this way, prescriber 560 can backtrack through connection steps that appear to have been competed successfully.

Detailed Description Text (87):
In operation, software modules on computers, such as remote computer 100, tunnel server 332, or management server 334, shown in FIG. 3, communicate to perform various management related tasks. For example, access 550 (FIG. 5) on remote computer 100 receives information from access service provider 720 (FIG. 7)

executing on management server 334 that is used to update local database 552 (FIG. 5). A communication infrastructure, called the delivery system, links the communicating computers. On each computer, a delivery module, such as delivery 572 (FIG. 5) on remote computer 100, delivery 620 (FIG. 6) on tunnel server 332, and delivery 710 (FIG. 7) on management server 334, provide other modules with access to this communication infrastructure. Together, these cooperating delivery modules make up the delivery system.

Detailed Description Text (88):
The delivery system provides communication services between software modules executing on the same machine as well as modules executing on different machines. The system provides secure communication between machines, and enforces a security policy for communication between modules executing on different machines. This security policy is based on a set of levels of trust, called rings. When communicating between machines, delivery uses the TCP/IP protocol suite to transfer data.

Detailed Description Text (95):
Referring to FIG. 18, a representative delivery module, delivery 1800, includes several elements. Delivery users 1805 interface with user message queues 1810 which hold inbound and outbound messages to delivery users 1805. When a delivery user 1805 sends a message, that is provides a message with an explicit address, that message is first stored in user message queues 1810 and then passed to a multiplexer 1820 and placed in an appropriate priority queue in multiplexer 1820. Multiplexer 1820 processes messages in priority order. If the message is addressed to a delivery user on the same machine, the message is passed back to user message queues 1810. If the message is addressed to a delivery user on another machine (that is, a delivery user that has registered with another delivery module) the message is passed to remote delivery 1860. If remote delivery 1860 does not have an active session with the remote delivery module, remote delivery 1860 first establishes a session with the remote delivery module using a procedure described below. If a session was already active, or once a new session is established, the message is transferred to the remote delivery module after appropriate security check (described below) are performed.

Detailed Description Text (97):
When delivery 1800 receives a message from a remote delivery module, remote delivery 1860 accepts the message, and after performing security-related checks on the message, as described below, passes the message to multiplexer 1820 where it is placed on the appropriate priority queue. Multiplexer 1820 then passes the message to sync handler 1830 to handle local delivery.

Detailed Description Text (98):
The delivery system implements a distributed security policy based of levels, or rings, of trust. The ring level is indicated by an integer in the range 0 to 3. The lower the ring number, the more trusted a user or system is. The system prevents disclosure of message to recipients at remote machines which are at higher ring levels (less trusted) than intended by a publisher of a message. In addition, the system prevents a sender of a message attributing a lower ring level to the message than the sender's own ring level. This prevents a user or system providing information to other modules that is unduly trusted.

Detailed Description Text (99):
Referring to FIG. 19, the security policy is implemented at several points on a path from a sender, delivery user #11805a to a receiver, delivery user #2, 1805b, indicated by points A-E (1910-1950). When delivery user #11805a provides a message to delivery #11800a, it indicates the source ring level. Delivery #11805a is aware, based on a prior authentication process that is described below, or that delivery user's true ring level. If delivery #11805a is attributing a source ring level to the message that is lower than it's authorized ring level, the message is blocked at point A 1910. If the message is a published, rather than sent, it is next passed to sync handler 1830a. A second security check is based on the requested ring levels of the subscribers, and the destination ring level specified by the sender. Messages are only directed to destinations that are authorized to the specified destination ring level or lower at point B 1920 on the path. If a message is to be sent from the

delivery #11800a to delivery #21800b, the destination ring level of the message must be no lower than the ring level of delivery #21800b. If this is not the case, then the delivery #21800b cannot be trusted with the message, and the message is blocked at point C 1930. Once the message is received by delivery #21800b, remote delivery #21860b checks that the source ring level specified in the message is no lower than the ring level to which delivery #1 is authorized. If the source ring level is too low, the message is blocked at point D 1940. Finally, multiplexer 1820b checks that the actual receiving delivery user 1805b is authorized at a ring level no higher than the specified destination ring level. If the ring level of delivery user #21805b is too high, the message is blocked at point E 1950. In this way, information in messages is never disclosed to systems or users that are less trusted than intended by the sender, and messages and not accepted from remote delivery modules with a specified source ring level that indicates that the message should be more trusted than the authorization level of the sending delivery module.

Detailed Description Text (111):
Referring to FIG. 21, the details of an authentication exchange, including determination of a session (encryption) key for use on that session, include a sequence of exchanges. Delivery a 2110 is the delivery module initiating the exchange, and delivery b 2120 is the delivery module with which delivery a 2110 wants to communicate. The labeled arrows in FIG. 21 correspond to messages sent between the delivery modules or between delivery b and the authentication service provider The label A corresponds to a username or other identifier or key of the delivery user initiating the session. N0 corresponds to a random number generated at delivery a 2110. The first step is for delivery a to send A and N0 to delivery b (2150). In response to receiving A and N0, the username and random number from delivery a 2110, delivery b 2120 sends back a random number, N1, that it generated (2152). The random numbers N0 and N1 form challenges to which each receiving delivery module must respond. In response to receiving N1, delivery a computes a one-way hash function H(P,N1) using a secret password, P, and the random challenge, N1. Any of a variety of previously agreed upon hash functions can be used, such as the commonly used the Message Digest 5 (MD5) hash function. Delivery a then sends the computed hash value to delivery b (2154). In order to determine whether delivery a truly knows the secret password P, delivery b would compute the hash value directly if it knew the secret password. However, in order to maintain security, the password for that user is kept by authentication server 750 and not distributed to the delivery services. Instead, delivery b passes the received A, N0, and H(P,N1), and the random challenge N1 that it generated, to authentication service provider 750 (2156). Authentication service provider holds a password, P.sub.A, for user A. If authentication service provider 750 determines that its password P.sub.A for user A is the same as the password P known to delivery a, it informs delivery b that user A has successfully authenticated. In particular, authentication service compares the received value of H(P,N1) to a value H(P.sub.A,N1) that it computes locally. If they match, then user A has successfully authenticated. In order to allow delivery a to authenticate delivery b, authorization service provider 750 also computes a response to the challenge value N0, H(P.sub.A,N0). Authorization service provider also computes a session key k.sub.A =H(P.sub.A,N0.parallel.N1), where N0.parallel.N1 is a bitwise or of random numbers N0 and N1. Authorization service provider 750 also computes C(P.sub.A,R.sub.a,R.sub.b), the ring levels of the user at delivery a and the current ring level of delivery b, R.sub.a and R.sub.b respectively, encrypted using P.sub.A. Authorization service provider passes back H(P.sub.A,N0), k.sub.A =H(P.sub.A,N0.parallel.N1), R.sub.a, and C(P.sub.A,R.sub.a,R.sub.b) to delivery b (2158). Delivery b passes H(P.sub.A,N0) and C(P.sub.A,R.sub.a,R.sub.b) back to delivery a (2160). Delivery a compares the received value H(P.sub.A,N0) to the value H(P,N0) it computes locally, and if they are equal, authenticates delivery b. By decrypting C(P.sub.A,R.sub.a,R.sub.b), delivery a knows the ring level of the user a delivery a and the ring level of delivery b, as known to authentication service provider 750. Delivery a then computes its value of the session key as k=H(P,N0.parallel.N1). Delivery a and delivery b now share a common session key that can be used for encryption of communication between delivery a and delivery b.

Detailed Description Text (113):
In FIG. 22, initially management server 334 has already started up and delivery 710 and authorization server 750 are in communication. This communication is secure since both modules are executing on a single, physically secure, machine.

Detailed Description Text (123):
In a related embodiment of the invention, rather than providing dialing information to a corporate communication system typically using the services of an ISP, the system can be used to provide dialing information to access the ISP itself without establishing communication with any particular corporation. In this case, the management server is coupled to the Internet and is operated by an ISP, or possibly multiple ISPs.

Detailed Description Text (124):
In another related embodiment, a management server operated by an ISP can provide dialing information related to access to the Internet through that ISP, an a management server at a corporation can provide information related to users at that corporation, and access points, such as tunnel servers, used to access a corporate network. In such an arrangement, an access module on a remote computer would receive some of the information for its local database from the ISP's management server, and some of the information from the corporation's management server.

Detailed Description Text (127):
Also, as shown in FIG. 24, alternative arrangements or a tunnel server and a firewall can be used. For example, as shown in FIG. 24(a), a tunnel server can operate outside a firewall, and provide services including authentication of remote users to the firewall. Alternatively, as shown in FIG. 24(b), a tunnel server can provide a second point of access between a LAN and the Internet, thereby avoiding congestion at the firewall.

Detailed Description Text (128):
In the described embodiments above, separates costs are stored for use of a particular access number and use of a particular tunnel server. Other alternative cost structures can also be used. For example, there are situations in which performance factors are in general dependent on the particular combination of POP and a tunnel server. For example, if a single ISP operates both a POP and provides the point of access for a tunnel server to the Internet, performance may be better than if one ISP operates a POP and a second ISP provides the tunnel server access to the Internet.

CLAIMS:

1. Software stored on a computer readable medium for causing a remote computer to perform the function of: establishing a data communication path between the remote computer and a computing resource including determining a plurality of access paths for communicating between the remote computer and the computing resource wherein the plurality of access paths includes a plurality of telephone access paths that each includes a dialed telephone channel to a different telephone access number associated with that access path, determining a cost for each of the plurality of access paths, wherein each of the access paths is associated with a cost function and determining a cost for each of the access paths includes evaluating the cost function associated with said access path, selecting a first of the plurality of access paths based on the cost for each of the access paths, and initiating establishment of communication over the selected first of the access paths.

6. The software of claim 1 wherein the software further causes the computer to perform the functions of: accepting an identification of a location of the remote computer; and wherein determining the plurality of access paths includes determining a plurality of access paths according to telephone charges associated with use of dialed telephone channels from the location of the remote computer to each of the different telephone access numbers.

8. The software of claim 1 wherein the software further causes the computer to perform the functions of: accepting a dialing database, including telephone access numbers; accepting an identification of the computing resource; and wherein determining the plurality of access paths for communicating between the remote computer and the computing resource includes retrieving information related to the identified computing resource from the dialing database.

17. The software of claim 1 further causing the remote computer to: accept credentials from a user of the remote computer, the credentials including an identification of the remote user; authenticate the user by using the credentials and an authentication service on another computer; and establish a management communication path to the other computer and accepting information including information for a dialing database over the management communication path; wherein determining the plurality of access paths for communicating between the remote computer and the computing resource includes retrieving information related to the identification of the remote user from the dialing database.

20. The software of claim 19 wherein the software further causes the first computer to: accept master dialing information; accept local information, including information related to computing resources accessible from the remote computer; and maintain the dialing database using the master dialing information and the local information.

24. A method for establishing a data communication path between a remote computer and a computing resource including: determining a plurality of access paths for communicating between the remote computer and the computing resource wherein the plurality of access paths include a plurality telephone access paths that each includes a dialed telephone channel to a different telephone access number associated with that access path; determining a cost for each of said access paths, including evaluating a cost function to arrive at a cost of communicating between the remote computer and the computing resource over each of said telephone access paths; selecting a first of the access paths based on the cost for each of the access paths; and initiating establishment of communication over the selected access path.

25. A method for distributing dialing information to remote computers comprising: accepting master dialing information; accepting local information, including information related to computing resources accessible from the remote computers; maintaining a dialing database, which includes telephone access numbers for access paths from the remote computers to the computing resources, using the master dialing information and the local information; establishing a management communication path to one of the remote computers, including authenticating the remote computer; and providing information from the dialing database to the remote computer over the management communication path, for use on the remote computer in selecting an access path between the remote computer and one of the computing resources accessible from the remote computer.

26. A communication system on a remote computer comprising: a user interface for accepting an identifier of a location of the remote computer; a means for determining a plurality of telephone access paths for communicating between the location of the remote computer and a computing resource, including a local database for storing telephone access numbers and cost factors for the telephone access paths; a means for evaluating a cost function for each telephone access path, the cost function for each telephone access path characterizing a cost of communicating between the location of the remote computer and the computing resource over that telephone access path; a means for selecting one of the telephone access paths in accordance with the result of evaluating the cost functions for each of the telephone access paths; and a communication interface for communication over the selected telephone access path.

27. A communication system comprising: a management computer, including a dialing database for storing an association of a plurality of calling locations and corresponding subsets of a plurality of telephone access numbers for accessing a computing resource, and for storing an association of the telephone access numbers and monetary and performance factors related to data communication over dialed telephone connections from the calling location to the telephone access numbers; and a plurality of remote computers, each including a local database for storing part of the information stored in the dialing database on the management computer; wherein each of the remote computers further includes software for causing the remote computer to determine, using information stored in the local database, a plurality of telephone access paths for communicating between the remote computer and a computing resource, evaluate a cost function for each of the plurality of telephone

access paths, the cost function for an access path characterizing a cost of communicating between the remote computer and the computing resource over that access path, select one of the plurality of telephone access paths in accordance with a result of evaluating the cost functions for each of the telephone access paths, and communicate over the selected telephone access path; and wherein the management computer further includes software for causing the management computer to accept communication from each of the remote computers, and to provide information in the dialing database to the remote computers.

33. A method for enforcing access policies for a plurality of classes of remote users comprising: maintaining an access database characterizing access paths from a plurality of remote locations to a computing resource; and distributing information from the access database to a plurality of remote computers, including distributing information to each remote computer such that software executing on a remote computer selects an access path from a remote location of the remote computer to the computing resource according to the class of the remote user of that remote computer.

34. The method of claim 33 wherein distributing information to the remote computers includes distributing different selection factors for different classes for remote users wherein the selection factors are used on the remote computers for selecting access paths from the remote computer to the computing resource.

WEST

Generate Collection Print

L32: Entry 6 of 16 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6396849 B1
TITLE: Systems and methods for multiple mode voice and data communications using intelligently bridged TDM and packet buses and methods for performing telephony and data functions using the same

Abstract Text (1):
Systems and methods by which voice/data communications may occur in multiple modes/protocols are disclosed. In particular, systems and methods are provided for multiple native mode/protocol voice and data transmissions and receptions with a computing system having a multi-bus structure, including, for example, a TDM bus and a packet bus, and multi-protocol framing engines. Such systems preferably include subsystem functions such as PBX, voice mail and other telephony functions, LAN hub and data router. In preferred embodiments, a TDM bus and a packet bus are intelligently bridged and managed, thereby enabling such multiple mode/protocol voice and data transmissions to be intelligently managed and controlled with a single, integrated system. A computer or other processor includes a local area network controller, which provides routing and hub(s) for one or more packet networks. The computer also is coupled to a buffer/framer, which serves to frame/deframe data to/from the computer from TDM bus. The buffer/framer includes a plurality of framer/deframer engines, supporting, for example, ATM and HDLC framing/deframing. The buffer/framer is coupled to the TDM bus by way of a switch/multiplexer, which includes the capability to intelligently map data traffic between the buffer/framer and the TDM bus to various slots of the TDM frames. Preferably, a DSP pool is coupled to buffer/framer in a manner to provide various signal processing and telecommunications support, such as dial tone generation, DTMF detection and the like. The TDM bus is coupled to a various line/station cards, serving to interface the TDM bus with telephone, facsimiles and other telecommunication devices, and also with a various digital and/or analog WAN network services.

Brief Summary Text (2):
The present invention relates to systems and methods for transmitting and receiving voice and data in multiple modes, and more particularly to systems and methods for multiple native mode voice and data transmissions and receptions with a communications system having a multi-bus structure, including, for example, a time division multiplexed ("TDM") bus, a packet bus, and a control bus, and multi-protocol framing engines, preferably including subsystem functions such as PBX, voice mail, file server, web server, communications server, telephony server, LAN hub and data router, and methods for performing telephony and data functions using the same.

Brief Summary Text (4):
Businesses, particularly small to medium size offices, typically have a need for a variety of voice and data communications. For example, a typical office might have a dedicated fax machine, using a dedicated or shared telephone line, one or more telephone lines for voice communications, perhaps coupled to a central or distributed voice mail system(s), and one or more computers or computer networks, often coupled to telephone lines via one or more modems. Many offices now use the Internet in some form for business communications or research or the like, often by way of a modem or modem pool coupled to individual computers.

Brief Summary Text (6):

FIG. 1 illustrates a conventional small office communication configuration. Voice communication system 1 typically is implemented by way of multiple analog trunks 16 from wide area network ("WAN") 18. WAN 18 often consists of a telecommunication network by way of a local telephone company or other telecommunications service provider. Analog trunks 16 may be directed through switching system 10, which may be a conventional PBX or similar telephone switch. Telephones 12 and voice mail system 14 are coupled to switching system 10. Often, dedicated analog line 16A is coupled to facsimile 44 for facsimile communications.

Brief Summary Text (10):
The present invention is intended to address various disadvantages of such conventional communication systems. The present invention provides various systems and methods, perhaps more succinctly a platform, by which voice and data communications may occur in multiple modes and various protocols, and more particularly systems and methods for multiple native mode voice and data transmissions and receptions with a communications/computing system having a multi-bus structure, including, for example, a TDM bus, a packet bus and a control bus, and multi-protocol framing engines, preferably including subsystem functions such as PBX, voice mail and other telephony functions, email and/or file server, Internet server, LAN hub and data router. With the present invention, a platform and various processes are provided in which a TDM bus and a packet bus are intelligently bridged and managed, thereby enabling such multiple mode/protocol voice and data transmissions to be intelligently managed and controlled with a single, integrated system.

Brief Summary Text (11):
In preferred embodiments, a computer or other processor includes a local area network controller, which provides routing and hubs and/or switches for one or more packet networks. The computer also is coupled to a multiple buffer/framer, which serves to frame/deframe data to/from the computer from a TDM bus. The buffer/framer includes a plurality of framer/deframer engines, supporting, for example, ATM and HDLC framing/deframing, and raw buffering of voice data or the like. The buffer/framer is coupled to the TDM bus by way of a multiple port or multiport switch/multiplexer, which includes the capability to intelligently map data traffic between the buffer/framer and the TDM bus to various slots of the TDM frames. Preferably, a DSP pool is coupled to one or more switch/multiplexer ports and/or the buffer/framer in a manner to provide various signal processing and telecommunications support, such as dial tone generation, DTMF detection and the like. The TDM bus is coupled to various line/station cards, serving to interface the TDM bus with telephone, facsimiles and other telecommunication devices, and also with various digital and/or analog WAN network services. The present invention provides a platform by which processing functions may be switched to provide support for a wide-range of network, vendor and application services.

Brief Summary Text (12):
With the present invention, a full PBX-type telecommunication system may be provided by way of the computer/processor and associated telephony hardware and software. Functions such as voice mail, automated attendant, call forwarding, hold, transfer, caller ID, conferencing and other telephony functions may be similarly provided. While supporting such telephony functions in their native mode primarily by way of the TDM bus, the computer/processor also supports concurrent packet data transmissions over the LAN subsystem and packet bus(es). As needed to efficiently support various voice/data communications in the particular office/work environment, the buffer/framer and switch/multiplexer provide a multi-protocol router functionality, enabling the TDM bus traffic and the packet bus traffic to be intelligently bridged and managed without degradation of each other, and without requiring translation or transcoding. With the present invention, the same WAN services may be intelligently managed and controlled for simultaneous voice, video, and data traffic.

Detailed Description Text (6):
Communications system 50 includes the functionality of what is known as a PBX (as will be described further). In preferred embodiments, communications system 50 is connected to a plurality of telecommunication devices, such as telephones 12, facsimile 44 and other suitable telecommunications devices and access and server

functions (such as private voice mail, recording devices, WAN service interface cards, etc.). What is important is that communications system 50 include interfaces for a plurality of telecommunications devices for the particular and complete office/work environment and infrastructure.

Detailed Description Text (7):
Communications system 50 is coupled to WAN voice/data services network(s) 58 through trunks 54. Voice/data services network(s) may include private line, local or long distance carrier networks, Internet, intranet and/or any other current or future WAN-type network services. Trunks 54 may consist of high, medium or low speed digital and/or analog lines, either public or private, and in certain preferred embodiments consist of high speed dedicated resources such as what are known as T-1, PRI (Primary Rate ISDN), ATM, VDSL, HDSL, ADSL, wireless, cascade, proprietary and/or twisted pair analog lines from a local telephone company. What is important is that communications system 50 is coupled to WAN services, trunks and the like in a manner that the user, service provider, administrator and/or algorithm has determined will provide adequate or required resources, on a cost-effective basis, for the particular office/work environment and operating conditions.

Detailed Description Text (14):
Coupled to TDM bus 78 are line, station, trunk, or other interface cards 82. Cards 82 provide CODEC, line interface, off-hook detect and other functions as are known in the art to support various telecommunication devices (such as telephones 12 and facsimile 44) and WAN-type network services (such as voice/data services 58) that are communicating with communications system 50 via TDM bus 78. In preferred embodiments cards 82 provide points of termination for a plurality of telephones 12, one or more facsimiles 44, and various T-1, PRI, ATM, analog and/or other WAN-type network services as determined by the particular office/work environment. Cards 82, under control of processor/system resources 70, may include points of termination for emergency or backup telephone services and the like, such as in the event of a power failure or to provide analog services in the event a dedicated resource such as a T-1 is unavailable for some reason.

Detailed Description Text (15):
Communication system 50 also may include fax modem 75, which, under control of processor/system resources 70, may process incoming/outgoing facsimile transmissions. In the preferred embodiment, fax modem 75 is coupled to TDM bus 78 as illustrated, although in other embodiments fax modem 75 may be coupled in alternative arrangements, such as to switch/multiplexer 74 and/or DSP 76.

Detailed Description Text (26):
At the server applications level, various software applications may be provided for operation in conjunction with the hardware illustrated, for example, in FIG. 3. Such software applications may include what are known as least cost routing ("LCR"), best quality of service ("BQOS") and bandwidth ("B/W") rules 21. LCR, BQOS and B/W rules 21 provide tables, information, rules and/or algorithms by which data and voice communications may be allocated and/or controlled with respect to, for example, the various types of voice/data network services that are available to communications system 50. Such information may include the current cost of utilizing various resources (based on time of date, amount of usage, integrated amount of usage over some period of time, etc.), and also priority rules for the various types of communications provided by communications system 50. For example, phone calls may be assigned a priority 1, facsimile calls a priority 2, VoIP calls a priority 3, facsimile over IP calls a priority 4, category 1 data communications a priority 5, and other data communications a priority 6. In preferred embodiments, the priority assignments may change by time of day or month, and/or the priority assignments may be different with respect to different network resources and the like.

Detailed Description Text (29):
Intelligent/dynamic B/W, service and resource management 31 is provided to effectively and efficiently control and allocate and de-allocate services and communications resources, such as in accordance with LCR, BQOS, B/W rules 21 (e.g., rules to enable lowest cost, highest quality or otherwise desirable management and control of network or other resources, etc.) or other applications 29 or the like. B/W management 31 also receives as inputs information indicating the total number

and types of network resources (of voice/data services 58, for example) that are available to communications system 50, and their status and availability at any given point in time. B/W management 31 may receive as an input, or may generate internally, information indicating how much of a measured usage resource may be available at a given point in time (for example, "frame relay," "private virtual channel" or other network services may be provided on the basis of a predetermined amount of data transmission per fixed time period for a fixed price, with additional charges for usage in excess of the predetermined amount, etc.). As more fully described below, based on the currently available and currently utilized services and resources, B/W management 31 may allocate and de-allocate such services and resources in a desired and/or cost efficient manner.

Detailed Description Text (31):
For example, data switching services may be provided such as by LAN/NDIS/DDI drivers 39 (LAN, NDIS and DDI being exemplary) through hardware modules such as switched Ethernet 45 and hub 47. Routing services may be provided such as through WAN drivers (specific network services such as PRI and T-1 being exemplary) through hardware modules such as T-1 module(s) 49, ISDN module(s) 51, central office-plain old telephone service (CO-POTS) module(s) 53, V.35 module(s) (it should be understood that various hardware modules may be utilized in accordance with preferred embodiments of the present invention, as desired to implement the various data switching, routing and other communications connections as may be determined by the needs of the particular office/work environment). PBX station services, such as automated attendant, reception, voice mail and the like, may be provided through station manager 43. Station manager 43 provides hardware for connection to various telecommunications devices, such as phones 12, facsimile 44, etc. In general, station manager 43 provides sufficient interface hardware in order to connect to the various devices that may be determined by the needs of the particular office/work environment.

Detailed Description Text (42):
As illustrated in FIG. 6, a party desiring to control the incoming and outgoing calls and/or station to station calls of the office ("attendant 1") may log-on and run the office attendant type program from one of the computers connected to the LAN connected to communications system 50. At step 100, attendant 1 may be required to enter an appropriate user name/ID and password in order to recognize attendant 1 as an appropriate user to assume control of the telephony functions of the office. A network or systems administrator may set up password control for parties authorized to run the office attendant type program. At step 102, in preferred embodiments the computer running office attendant type program has downloaded to it the current telephone subscriber directory such as over packet bus 80A or 80B of FIG. 3 (e.g.: a complete listing of the telephone subscribers; extensions; status information such as do not disturb, forward and forwarding information, forward to voice mail, hunt group information, etc.) from communications system 50. In this manner, the computer or computers running the office attendant type program may locally contain current subscriber information for controlling the incoming and outgoing calls of the office. In preferred embodiments, communications system 50 automatically determines when subscriber information changes, e.g., a subscriber has been added to or deleted from the telephone directory, or an extension has changed, or a subscriber's status information has changed, or any state associated with communications system 50, etc., in order that updates may be timely made available. In such embodiments, computers running the office attendant type program may be updated promptly and automatically by communications system 50 so as to contain current subscriber information on an ongoing basis to more efficiently control telephony operations of the office. It also should be noted that in preferred embodiments the subscriber information also may include other information, such as the email address and extended directory information including personal information manager ("PIM") information of the particular subscriber and network identification for a computer associated with the particular subscriber. With such information, net messages or other communications with particular subscribers may be facilitated as more fully described herein.

Detailed Description Text (43):
It also should be noted that this subscriber download concept is applicable in various forms to all computers coupled to communications system 50. For example,

communications system 50 includes information regarding all users registered in the PBX (i.e., all users having a telephone extension and/or computer coupled to communications system 50 such as over the LAN or WAN). Thus, in the event of a subscriber directory change, communications system 50 may "broadcast" updated subscriber directory information to all computers coupled to communications system 50, or, in alternate embodiments, communications system 50 sends a net message, email or other message to such computers coupled to communications system 50 that prompts the users of such computers to the availability of the subscriber directory update (e.g., the remote computers receive a message indicating the availability of the subscriber directory update, which preferably includes an "accept" icon and a "reject" icon, thereby enabling the user to receive or not receive the update as he/she may desire).

Detailed Description Text (59):
In accordance with preferred embodiments of the present invention, in the event of a failed transfer, for example in case the extension to which the call is being transferred is busy, a window preferably is automatically displayed on the computer running the office attendant type program. An exemplary window 208 is illustrated in FIG. 9B. As illustrated, display 210 may display a descriptive message, such as "line busy," "do not disturb," etc. Preferably, a number of icons also are simultaneously displayed to aid the office attendant type program user in processing this call. Hold icon 212 may be used to place the caller on hold. Message icon 214 may be used to initiate a net message to the party to whom the call is to be transferred. Voice mail icon 216 may be used to direct the call into the voice mail of the party to whom the call was to be transferred. Cancel icon 218 may be used to cancel the transfer operation. With such an automatically generated window 208, the office attendant type program user is presented with options to more quickly process such calls, again preferably with a single or very few clicks of the mouse or pointer.

Detailed Description Text (61):
In such embodiments, the called party may decide to terminate his/her existing call and accept the call from the party being transferred, such as by clicking on accept icon 224. Alternatively, the called party may decide to have the call from the party being transferred wait, such as by clicking on wait icon 226. The particular user being called preferably has the option to configure his extension to accept parked calls or to not accept parked calls. The particular user also preferably has the option to select an allowed parking time before the call is returned to the user running the office attendant type program. Thus, a transferred call may be temporarily parked, with an appropriate message displayed on the computer of the called party, with the parked call either accepted by the called party clicking on accept icon 224, returned to the user running the office attendant type program or forwarded to voice mail after a parking time out time has elapsed, or the call held longer than the allowed parking time by the called party clicking on wait icon 226. In certain embodiments, clicking on wait icon 226 enables the call to be parked indefinitely, while in other embodiments a second, longer and preferably user configurable parking time is enabled (thus preventing a called from being held for an indefinite period of time). If a time out time is exceeded, preferably the call is returned to the user running the office attendant type program or forwarded to voice mail, and still preferably an audible tone or sound is periodically emanated from the computer of the called party while the call is parked, thereby providing a subtle reminder of the existence of the parked call. In certain embodiments, users have the ability to mute or lower the volume of the reminder sound, such as by way of an additional icon in window 220. In all preferred embodiments, users have the ability to configure and select the particular options described herein that the particular users may desire.

Detailed Description Text (63):
It should also be noted that, in the event of a particular user extension being dialed directly without going through the office attendant type program, a window such as window 220 of FIG. 9C may be displayed on the computer of the called party, either automatically for all calls, or only in the event that the called party has put his telephone on do not disturb, but has configured his extension to receive a message notification of calls, or in the event that the called party is on the line. In such embodiments, communications system 50 may generate such a window by a

suitable message sent over by packet bus to the user's computer. In such embodiments, communications system 50 may simultaneously ring a user's extension and notify the user of the call with a net message, with the call being accepted, parked or forwarded to voice mail such as described earlier. Of course, in the event that a user previously configured his extension to be automatically forwarded to another extension or location or to voice mail or the like, then communications system 50 preferably takes the programmed action directly. As an illustrative example, a user may configure his extension so as to route all calls to another extension or to a local or long distance telephone number. Such a user also may configure his extension so as to route all calls as voice over IP ("VoIP") calls. In the later situation, processor/system resources 70 and/or DSP 76 may process the incoming voice information (received through the appropriate station card 82 and via TDM bus 78, etc.) into appropriate IP packets, which may then be routed, for example, through an HDLC framer/deframer 73B, through switch/multiplexer 74, over TDM bus 78 and out over a designated IP connection via WAN services 58, etc.

Detailed Description Text (66):
FIG. 10B illustrates net message window 240 that may appear on the computer of the recipient. The recipient is presented with the net message in window 242, and may close the net message by clicking icon 244. Alternatively, net messages may be stored for archival purposes or later viewing, and in alternative embodiments net messages also include a reply icon which may be clicked in order to bring up a window in which a reply message may be typed. In such embodiments, an office attendant type program user may inform the recipient, for example, of a particular caller, and the recipient may inform the office attendant type program user, for example, that the caller should be directed to a particular individual or department or processed in a particular way (directly to voice mail, call terminated, etc.). With such embodiments, packet bus or other messages may be readily exchanged in a manner to more readily facilitate telephony management, etc.

Detailed Description Text (78):
It also should be noted that an office attendant-type program also may be run from a location remote from communications system 50, such as on a computer coupled to WAN services network 58 of FIG. 3. In such embodiments, a remote computer coupled to communications system 50 over a WAN network connection may run the office attendant-type program and remotely control the telephony functions of the office, in a manner such as described previously herein. Thus, control of telephony functions may be effectively performed in the office or remotely from the office, with control passed from computer to computer in an efficient and desired manner. Additionally, the user of the remote computer may run an office attendant-type program or a companion program as described elsewhere herein, and from such remote location be coupled to communications system 50 and remotely reconfigure the telephony and/or voice mail settings for the particular user. As an example, the remote user may use the remote computer in order to direct telephone calls to his/her extension to voice mail, or alternatively to have such calls forwarded to another extension or to a remote telephone number. With such embodiments, particular users may remotely access communications system 50 and, for example, control the forwarding of calls to an internal or remote location. As a particular example, a user using a notebook computer or PDA, etc., may couple to the Internet or WAN, etc., from a remote location, and direct that telephone calls to his/her office extension be forwarded in a desired manner (e.g., off-premise call forwarding, etc.). With the user able to access communications system 50 and remotely set and store PBX-type settings remotely, a variety of desired reconfiguration options are presented to the user.

Detailed Description Text (80):
In preferred embodiments, communications system 50 may dynamically associate physical telephones 12 with particular user extension numbers. In certain respects, this may be considered like a "DHCP" (described elsewhere herein) for physical telephones. For example, a system administration may run a configuration/administration program (such as described elsewhere herein) and configure an extension number (e.g., 200) for a particular user, including associated parameters for such user, such as telephony and voice mail options (e.g., user forward settings, including off premise call forwarding, busy forward settings, ring-no-answer forward settings, time of day forward settings, display name for

telephones displaying caller names, etc., whether the telephone is configured to be a telephone for a user running an office attendant-type program, etc.). At this time, the system administrator may or may not assign a physical telephone to that extension. Thereafter, the system administrator may notify the user that his/her extension number is 200. The system administrator also has the ability to enable and/or assign physical telephones. In the event that the system administrator has not assigned a physical telephone to that user, the user preferably has the ability to assign a physical telephone to his/her extension. For example, the user may pick up a telephone that has been enabled, and preferably does not have an extension assigned to that telephone, and the user enters a special code, e.g., numbers that communications system 50 recognizes as a request to assign a physical telephone. In certain embodiments, communications system 50 audibly informs (such as using DSP 76) the user of the status of that physical telephone (e.g., enabled or disabled, presently assigned to an extension, etc.). Thereafter, the user preferably is prompted audibly to enter his/her extension number. Optionally after a confirmation prompt, communications system 50 then assigns that physical telephone to the particular user. Still optionally, if the particular user extension is already assigned to another physical telephone, then communications system 50 un-assigns the other physical telephone at the time a new physical telephone is assigned to the particular user/user extension.

Detailed Description Text (82):
Additionally, as previously described communications system 50 may serve as an email server or otherwise serve to distribute email to particular computers (such as computers 24) coupled to communications system 50. Thus, communications system 50 can store information indicating that a particular user or users have received email. In such embodiments, communications system 50 preferably provides a visual or audio indication to the user that he/she has email. As illustrative examples, a special dial tone or message may be generated (such as with DSP 76) and presented to the user's telephone so that, when the user picks up his/her telephone, the special dial tone or message alerts the user that he/she has email (which also may include a special tone or message indicating that the user has voice mail). As one example, the tone or message may be a particular sound, but preferably is an audible message such as "you have email," or "you have voice mail and email" or "you have voice mail," etc. In the event that communications system 50 is implemented with telephones 12 having message indicator lamps, a particular lamp or blinking sequence may be used to indicate that the user has email, voice mail or both, etc. In all such embodiments, users may be desirably informed that they have email and/or voice mail with their telephony device (e.g., telephone).

Detailed Description Text (83):
As described elsewhere herein, communications system 50 may serve to provide email services to particular users with telephone extensions associated with communications system 50, etc. In addition, communication system 50 also provides a platform (such as with processor/system resources 70) on which various management, administration or other types of applications may be run (exemplary such applications are described elsewhere herein). In one embodiment, various WAN and other information is provided using what is known as a SNMP-type protocol; as is known in the art, SNMP stands for Signaling Network Management Protocol, which is a protocol/method by which network management applications can query or request information from a management agent (such as are implemented in the present invention with processor/system resources 70 and appropriate software, etc.). A novel aspect of such embodiments of the present invention is that the voice mail system of communications system 50 also is implemented in a manner to provide voice mail related information in an SNMP-type form. Thus, in accordance with such embodiments of the present invention, communications system 50 stores a variety of information relating to voice mail, such as information relating to the status of the voice mail system, failure or alarm-type information, usage statistics, etc. In such embodiments, any tool or application that is SNMP compliant can access and view such voice-mail related information. Exemplary voice-mail-related information that may be made available via SNMP to an SNMP compliant tool or application is set forth in Table 1. With such embodiments, network (WAN and LAN, etc.) and PBX information along with voice mail-related information may be desirably provided using SNMP to a variety of SNMP tools and applications.

Detailed Description Text (88):
Yet another embodiment of video conferencing in accordance with the present invention is described with reference to FIG. 13C. As illustrated, computer 24 is coupled to communications system 50 over packet bus 80A (see, e.g., FIG. 3). Computer 24 includes camera 24A and preferably a microphone and speaker. Video and audio information preferably is coupled between communications system 50 and computer 24 through an appropriate packet standard, for example what is known as H.323. Referring again to FIG. 3, in such embodiments packetized video information is provided from computer 24 to communications system 50 over packet bus 80A. Processor/system resources 70 processes the packetized data stream (e.g., de-packetizes the data stream), which preferably now is in a suitable form/protocol (such as TCP/IP) for transmission to a remote computer running a compatible video conferencing program. As illustrative examples, the video data stream may be directed by processor/system resources 70 to fax modem 75 and coupled to a remote computer, or the video data stream may be directed by processor/system resources 70 to an HDLC framer/deframer 73B, to switch/multiplexer 74, to TDM bus 78, to an appropriate station card 82 and to WAN services network 58 via trunk 51 to which is coupled one or more remote computers for completing the video conference. It also should be understood that one or more such computers desiring to establish a video conference also may use an Internet connection established with the aid of what is known as an ILS (or Internet locator service) dynamic directory, a real time directory server component, which serves to aid "user to IP mapping" for establishing desired point-to-point connections for video conferencing.

Detailed Description Text (97):
Communications system 50 increases the efficiency of office communications and provides businesses a competitive edge by integrating the following voice, data, and communications functions into one remotely manageable platform: PBX; Voice mail; Automated attendant; Computer-telephony applications server; Channel bank; Router; CSU/DSU; LAN hub; Remote access server; and Modems.

Detailed Description Text (110):
Communication system 50 is easy to install, manage, and use. Some of the features making communication system 50 easy to install, manage, and use are its web-based management for remote configuration, diagnostics, and health monitoring, remote software upgrades, rapid installation, customizable management levels, and full SNMP instrumentation for voice and data. These features simplifies management tasks by using a single, consistent management interface for voice and data infrastructure, reduces personnel costs by leveraging centralized technical resources to manage remote offices, minimizes downtime and on-site visits through extensive tools for remote troubleshooting and diagnostics, ensures system integrity by flexibly addressing different access requirements for system administrators, enables a user to reduce support costs by distributing simple, repetitive tasks such as moves, adds, and changes to office personnel, leverages your existing SNMP infrastructure to manage both voice and data capabilities on the communication system 50, allows the user to save money by performing software upgrades from a central location, and saves valuable time and money because the system can be installed and configured quickly.

Detailed Description Text (122):
PBX and the office attendant type program application are an integral part of the communications system 50. Other Communications system 50 software components include the following: Data Communications Services; Voice Mail and Auto Attendant applications; and Remote Management System.

Detailed Description Text (123):
With Communications system 50, higher productivity with voice mail and automated attendant services can be achieved. Communications system 50 voice mail and auto attendant services help an office increase productivity by allowing people to share information without time or distance constraints. Customers can leave messages at any time of day or night, with the assurance that the messages will be delivered. Whether an office personnel is in the office or on the road, any office personnel can access messages instantly from any phone in the world.

Detailed Description Text (124):

In addition, communications system 50 voice mail services allow a user to access the user's voice mail messages via the user's favorite e-mail application. Communications system 50 voice mail application is built with full support for open industry standards--including IMAP4 e-mail application compatibility for remote voice mail retrieval, and WAV sound file format for ubiquitous message playback using the most popular operating systems.

Detailed Description Text (126):
The following are exemplary communications system 50 voice mail and auto attendant Specifications. Voice mail features include the following: Up to six concurrent voice mail sessions; Approximately 67 hours of storage; No additional hardware required; Interruptible prompts; and Password protection. The voice message handling feature includes: New message retrieval; Save messages; Listen to deleted messages before you hang up; Hear message time stamp and duration; Forward message; Reply to message; Skip message; Go to end of message; Backup and forward 5 seconds; Pause/resume listening; and Pause/resume recording.

Detailed Description Text (127):
The versatile message notification features include: Stutter dial tone; Lamp indication; and IMAP4 e-mail retrieval. Next, the auto attendant features include: Customizable greetings; Time, day-of-week, and holiday scheduling; Automated call routing (individual extensions and hunt groups for departmental routing); Audio-text mailboxes; Dial by name; Multilevel menus; and Single-digit menus.

Detailed Description Text (128):
The voice mail and auto attendant applications are an integral part of communications system 50. Other communications system 50 software components include: PBX services; office attendant type program computer-telephony application; Data Communications Services; and Remote Management System.

Detailed Description Text (130):
Communications system 50 data communications services provide built-in services for local area networks, connecting branch offices to headquarters, and providing remote access and Internet connectivity to its employees. In addition, the data communications services allow offices to create virtual private networks (VPNs) to save money on remote access and interoffice connectivity. Further, an office can save significant money by integrating both voice and data traffic over the same T1 access circuit. The built-in multiplexer passes data traffic to the data communications services for processing; the remaining voice traffic is passed directly to the PBX.

Detailed Description Text (133):
Virtual private networks lets a user use IP packet networks, such as the Internet, to provide secure connections between remote users and their corporate networks, without the expense of a dedicated private network. Communications system 50 offers a flexible and comprehensive solution, based on the Point-to-Point Tunneling Protocol (PPTP), for creating VPNs.

Detailed Description Text (136):
Data communications services are an integral part of communications system 50. Other communications system 50 software components include: PBX services; communications system 50 computer-telephony application voice mail and auto attendant applications; and Remote Management System.

Detailed Description Text (141):
(2) SNMP: Both the voice and data aspects of communications system 50 have been SNMP instrumented, including key application services such as voice mail and PBX.

Detailed Description Text (144):
(5) Trace manager: A complete log of all system activity, the trace manager provides useful information such as real-time call progress, WAN protocol traces, frame relay management information, and voice mail activity to facilitate troubleshooting.

Detailed Description Text (145):
Below are the specifications for an exemplary communications system 50 Remote

Management System: Rapid installation: less than 30 minutes; Remote software upgrades; Minimal technical expertise required; Robust, low-maintenance platform; Architected for high availability; Self-diagnostics to ease management burden; Remote management via digital trunks and over embedded 56Kbps modems; and Centralized password facility. A Remote Management Console of the present invention includes the following features and benefits: Web-based console that manages all voice and data services; Management of a system in a network over any TCP/IP connection; Multiple administrative levels (customizable); Password protection; Support for remote moves, adds, and changes; Monitoring and diagnostic utilities; Chassis view that provides an at-a-glance view of system status, including LED states; Graphical user interface that is easy to learn and use; Extensive online help; and Runs on Windows 95 and Windows NT, using Internet Explorer 4.0 or Netscape 4.0.

Detailed Description Text (146):
The SNMP features include the following: Full SNMP instrumentation for voice and data; Support of standard enterprise network management stations such as HP OpenView and Sun NetManager; SNMP standards: SNMP (RFC 1157), Structure and Identification of Management Information (RFC 1155), Concise MIB Definitions (RFC 1212), MIB-II MIB (RFC 1213), Traps (RFC 1215); Standard MIBs: Frame Relay DTE (RFC 1315), T1/E1 Interfaces (RFC 1406), Repeater (RFC 2108), Microsoft HTTP, Microsoft LAN Manager, Microsoft RIPv2, Microsoft OSPFv2; Private MIBs: T1 extensions, station module, voice mail Call detail recording (CDR); Complete record of all voice and data calls placed or received; Standard file format for import into CDR applications; and Remote analysis of CDR information without a dedicated workstation.

Detailed Description Text (149):
The communications system 50 Remote Management System is an integral part of the preferred communications system 50. Other communications system 50 software components include the following: PBX services; Communications system 50 computer-telephony application; data communications services; and voice mail and auto attendant applications.

Detailed Description Text (159):
What is important to note is that administration/configuration of communications system 50 may be remotely performed via an IP or similar connection, preferably with a browser-type application, and preferably using the HyperText Transfer Protocol ("HTTP") or similar protocol (as known in the art, with a protocol such as HTTP a connection between a client and a server is severed once a request or a response message has been transmitted). In such preferred embodiments, HTTP commands may be used to remotely administer, configure and diagnose communications system 50 in a desirable and flexible manner. It should also be noted that the use of HTTP commands in such a manner to administer, configure, etc., WAN resources (e.g., T-1 cards or resources), PBX and telephony resources (e.g., station cards, voice mail), and LAN resources (e.g., ethernet or other network cards/resources) enables remote control and monitoring of communications system 50 in a flexible and desirable manner. In particular, if a security arrangement known as a "firewall" is implemented in conjunction with communications system 50, the use of such HTTP commands to configure a WAN service (for example) may be more readily accomplished in that most firewall systems utilize ports that allow HTTP communications/traffic, which thereby reduces conflicts with the firewall security system. In effect, remote processing may be accomplished by HTTP "tunneling" into communications system 50 with an IP-type connection, etc.

Detailed Description Text (161):
It also should be noted that such embodiments preferably operate on the basis of "transactions." Preferably, the remote computer or client coupled to communications system 50 using a session implemented with HTTP "tunneling" establish a transaction-based interaction. In accordance with such embodiments, the client initiates a transaction using, for example, Java programming remotely, such as over the Internet, preferably using what is known as a private virtual network or private virtual channel connection. The particular transaction or operation (such as described elsewhere herein) are initiated by a client and proceed until completion, at which time the results of the transaction are made known to the client, or else the client has the option prior to completion of the transaction of "rolling back"

or canceling the transaction in the event that the client user determines that something is wrong or incorrect with the transaction, etc. Preferably, the software on the communications system "server" prompts the client with an option to accept, modify or roll-back the transaction. In preferred embodiments, the client-server session may process one or a series of such transactions. With such a transaction-based system, remote commands and operations may be performed in a more secure manner between the preferably Java client and server, all of which is preferably achieved using HTTP tunneling as previously described.

Detailed Description Text (162):
Referring again to FIG. 15, various icons are illustrated for remote access by a user desiring to remotely administer/configure communications system 50. By clicking appropriate icons, various system administration/configuration functions may be implemented. As illustrated, general administration functions may include or relate to: log off, diagnostics, help, chassis view (described in greater detail later), general settings, software versions (enabling a viewing of a registry of software modules and releases, etc., installed on the particular communication system 50), call detail report, restart/reboot, password administration, SNMP configuration, system backup/restore, disk array configuration, access permissions, SNMP alarms, software upgrade, date and time, etc. As illustrated, PBX and voice mail administration functions may include or relate to: extension configuration, auto attendant and voice mail, first digit table, hunt groups, station ports, local TAPI configuration, CTI speed dial numbers, etc. As illustrated, data administration functions may include or relate to: IP network settings, IPX configuration, RRAS routing (routing and remote access service), network services and adapters, etc. As illustrated, trunk administration functions may include or relate to: trunk groups, T-1 trunks, trunk access profiles, analog trunks, frame relay, etc.

Detailed Description Text (163):
What is important to note is that, in such preferred embodiments, various icons are presented so that a remote person may conveniently select via an appropriate and intuitive icon an applet to achieve the desired function or operation, and which may conveniently be used to configure and administration the communications system and configure PBX, voice mail, LAN and IP network connections, trunk groups, T1 trunks, frame relay, etc. In accordance with such embodiments, a single user interface, remotely viewable, may be used to access and administer, etc., voice, data, LAN, WAN services and applications, etc.

Detailed Description Text (170):
As illustrated in FIG. 16C, window 382 may be presented in order to configure station ports of a station card (again, either by icon selection or selecting a station card in chassis view, etc.). Also as illustrated, the state of particular stations (e.g., enabled or disabled), phone type (e.g., caller ID, basic, etc.), mail waiting indicator (MWI) (e.g., stutter the dial tone, light a lamp on the phone, etc.), operation mode (e.g., operate as a station, direct to voice mail, etc.). As described earlier with respect to FIG. 16B, with intuitive point and click type operations, various station cards may be selected (including multiple stations that may be selected as a block, etc.) and configured remotely and in an intuitive manner.

Detailed Description Text (174):
As illustrated in FIG. 17A, various icons may be presented in order for a remote user to perform remote diagnostics on communications system 50. Such icons may be used to present, for example, various "DOS prompt" type commands (e.g., Ping, ARP, route print, net stat, host name, trace route and IP config). Icons also may be presented for more advanced diagnostic-type operations, such as trunk monitor, link monitor, voice mail monitor, station monitor and trace monitor. Various of these diagnostic operations will now be more fully described.

Detailed Description Text (176):
In accordance with preferred embodiments, advanced remote trace monitoring also may be provided. FIG. 17E illustrates window 396, which may be used to display trace information from various software components, drivers, etc. in communications system 50. The level and type of trace information that is remotely provided may be desired controlled in accordance with preferred embodiments of the present invention. FIG.

17F illustrates window 397, in which a first level of tracing information (e.g., "standard") that may be provided is selected. As illustrated, the remote user may select various components to have trace information provided in the trace monitor window. FIG. 17G illustrates window 398, in which a second, higher level of tracing information (e.g., "advanced") that may be provided is selected. As illustrated, the remote user may select various software components, such as those related to automated attendant, voice mail, connection manager, DSP manager, T-1 drivers, LAN drivers, frame relay drivers, etc., and may also select various trace filters to more precisely control the trace information that is provided. FIG. 17H illustrates window 399, in which certain timing and mode information may be selected. As illustrated, window 399 may be used to provide that tracing information is presented in real time or stored to a file, with control preferably provided for the number of entries that are displayed, poll interval, etc. For trace entries stored in a file, start and end time search parameters also may be selected.

Detailed Description Text (184):
As described elsewhere herein, various voice mail type options may be presented to users of such communications systems in accordance with the present invention. One such advantageous voice mail option provided in accordance with preferred embodiments of the present invention include advanced email or voice mail-type broadcasts of desired messages. A user may decide to send a voice mail or email to some or all users of the communication system. With a suitable office attendant-type or companion-type program, for example, a user may select from a group list, etc., a desired group of persons to receive the communication. A broadcast voice mail, for example, could be input through the user's telephone in a conventional manner, and routed (see FIG. 3) through, for example, DSP 76 (via TDM bus 78, switch/multiplexer 74, etc.) which converts the voice mail message into an suitable data format, such as what is known as a WAV file, etc., and then sent via (for example) packet bus 80A and/or 80B to a plurality of computers. Communications system 50 also, for example, can record which users have received or not received the communication so that users may later receive the communication (such as when they log on at a later time). In addition, communications system 50 also has the capability to parallely process the communication as a message that is to be sent to persons via, for example the Internet. Using an HDLC framer/deframer as is provided in accordance with the present invention, a user may generate a voice mail or email communication that the communications system sends as packetized data over the LAN to recipients recognized to be users having a computer on the LAN, while generating a suitable HDLC or ATM framed communication to recipients who are reachable over the WAN, such as over the Internet or other IP connection, etc.

Detailed Description Text (185):
Described elsewhere herein are embodiments in which visual representations of pink slips or yellow stick-ons are generated to represent net messages, etc. This concept, in other embodiments, is extended also to voice mail and email messages. While not expressly illustrated, it should be understood that the present invention includes the ability to convert voice information (including voice mail type messages) into a suitable data format so that it may be delivered over the WAN or LAN to various computers coupled to communications system 50. Similarly, communications system 50 has the capability also to serve as an email server (in addition to other functions, as described elsewhere herein). Thus, in conjunction with a suitable program running on particular computers coupled to communications system 50, voice mails may be presented as data files to the various particular computers, and emails and net messages may similarly be presented to the various particular computers (such as described elsewhere herein). In certain alternate embodiments one, two or three visual "stacks" may be presented, for example, with one stack constituting a visual representation or a stack of voice mails (with suitable icons for play, pause, backward, forward, delete, file, freeze/hold, etc., as well as other icons analogous to those described for net messages), with a second stack constituting a visual representation of a stack or net messages (such as described elsewhere herein), and/or with a third stack constituting a visual representation of a stack of email messages (with icons similar to those described for net messages, etc.). Such stacks preferably may be minimized or expanded, and desirably provide a unified visual interface for a variety of communications, etc.

Detailed Description Text (187):

It also should be noted that, in preferred embodiments, DSP 76 is coupled to switch/multiplexer 74 in a manner so that it may "tap" into the various TDM data streams. This provides a significant improvement over systems in which data streams must be directed into a resource such as DSP 76, and then sent from DSP 76 over a separate channel, etc. (thereby utilizing two channels, etc.). In such embodiments, DSP 76 can tap into or monitor data streams on particular TDM channels and provide, for example, processing to accomplish recognition (voice or speech, etc.), detection (such as of a fax or modem call, etc.), compression (including compression, transcoding, streaming and storing, etc.), packetizing (such as to prepare a data format such as for an email, etc.). In one illustrative example of such embodiments, communications system 50 may be programmed so that particular users (e.g., president, technical support, warranty claims line, etc.) automatically have voice mails stored as voice mails and also as an email or other data form. Thus, a voice call may be directed into voice mail, while DSP 76 concurrently processes the voice data stream into another form (e.g., email, data file, etc.), which may be stored, sent over the WAN or LAN, etc. Having DSP 76, and particularly configured (such as with switch/multiplexer 74) so as to tap into the various channels, provides significant advantages in a variety of applications.

Detailed Description Text (191):
Preferably, memory 424 receives and stores via bus interface 420 a variety of information regarding the status and operation of communications system 50. For example, memory 424 may store power-on self test data (i.e., status, trace or other information generated during power-on, boot-up, etc.), SNMP data for the PBX, WAN resources, voice mail, LAN resources, etc.), monitor or trace data (such as described elsewhere herein). Preferably, module 416 receives periodic updates from communications system 50, including information sufficient to debug, reboot, etc., communications system 50. Various trace, monitoring, diagnostic or other information may be made available to module 416 for storage in memory 424.

CLAIMS:

1. In a system for managing voice and data communications of an office, wherein the system is coupled to at least one telecommunications network, the office having a plurality of computers coupled to the system over at least one packet bus and a plurality of telephones coupled to the system over at least one time division multiplex (TDM) bus, wherein the at least one TDM bus is selectively coupled to the at least one packet bus and the at least one telecommunications network, wherein the system provides voice and data communications to a plurality of users in the office, wherein associated with at least a first user is at least a first computer and at least a first telephone, a method comprising the steps of:

selectively coupling packet-based communications to or from the at least one packet bus from or to the at least one telecommunications network via the at least one TDM bus;

receiving telephone calls for users in the office from the at least one telecommunications network, wherein voice communications occur over the at least one TDM bus;

recording in voice mail of the system one or more voice messages for the first user based on one or more received telephone calls and coupled to voice mail via the at least one TDM bus;

receiving one or more electronic messages for the first user from the at least one telecommunications network via the at least one TDM bus;

storing one or more electronic messages for the first user in the system;

providing an indication to the first user via the first telephone that the first user has received one or more electronic messages for the first user; and

providing the one or more electronic messages to the first user over the at least one packet bus;

wherein the system provides voice communications from the one or more telephones over the at least one TDM bus and packet-based communications over the at least one packet bus, wherein voice communications that stay in a circuit-switched form in the system occur over the TDM bus and the at least one telecommunications network, and wherein packet-based communications are concurrently coupled to the at least one telecommunications network via the TDM bus.

L21: Entry 3 of 4 File: USPT May 7, 2002

DOCUMENT-IDENTIFIER: US 6385653 B1
TITLE: Responding to network access requests using a transparent media access and uniform delivery of service

Brief Summary Text (11):
After performing the above authentication step AAA server 26 performs an authorization step by responding with either a RADIUS access accept packet 36 or access reject packet 38. If an access accept packet 36 is returned, network access service 16 will also need to provide an IP address by seeking the services of a DHCP server 40 (dynamic host configuration protocol). This requires network access service 16 to generate a DHCP discover packet 42 having the user ID, among other things.

Brief Summary Text (12):
Upon receipt of DHCP discover packet 42, DHCP server 40 obtains the user ID contained within packet 42 to obtain a user record 44 from a user record database 46. User record 44 is then used to determine whether a predetermined IP address should be returned to network access service 16 or whether an IP address should be obtained from a pool of IP addresses. The IP address obtained by DHCP server 40 is then sent to network access service 16 using a DHCP offer packet 48.

Brief Summary Text (13):
Upon receipt of DHCP offer packet 48, network access service 16 obtains the IP address from packet 48 and encapsulates it as a RADIUS packet 50 and sends it to host 14 via modems 20 and 18, respectively. Upon receipt of RADIUS packet 50, host 14 returns an accounting start packet 52 to network access service 16, triggering an accounting process to begin.

Brief Summary Text (14):
Access point 10 is also shown supporting an ADSL access method. An ADSL compliant client 60 must not only obtain AAA and DHCP services from servers 62 and 64, respectively, as in the dial-up access method discussed above, but it must also first translate a private address used by an ADSL modem 66. This requires providing and maintaining separate databases 68 and 70. Moreover, the user records stored in database 68, must also include attributes specific to information required by the ADSL modem such as a service type attribute 68. The service type attribute includes a list of services in which the user is subscribed, such as the VPDN (Virtual Private Dial-up Network) service.

Brief Summary Text (15):
Access point 10 is also shown supporting a cable modem access method via a client 80. Supporting a cable modem network access method does not require a host, such as host 14, to obtain AAA and DHCP services. Instead, an IP address and authentication services are obtained when host 14 sends a request for registration services packet 82 using the MCNS (Multimedia Cable Network System) protocol.

Detailed Description Text (9):
Address procurement service component 128 may be provided using a DHCP (dynamic host configuration protocol) server, such as when communication system 120 is implemented using the Internet as the primary network backbone. DHCP servers are

available from Software.com of Los Angeles, Calif. AAA and DHCP servers traditionally rely on the RADIUS and DHCP application protocols, respectively, for communication.

Detailed Description Text (23):
If a cable modem access method i s supported, a protocol handler is provided that communicates with a cable modem client, such as MCNS protocol handler 174, and is configured to follow a set of steps defined by state manager 170. The steps direct MCNS protocol handler 174 to provide the necessary states required to process a task encapsulating an access request packet received from a cable modem client, such as cable modem client 144. Thus, for each protocol used by a particular access method, the present invention provides a protocol handler compatible with the protocol and a set of steps which have been configured to direct a respective protocol handler to provide the necessary states required to respond to an access request based on a supported access method. Protocols other than those described are also supported, such as TACAS+, Diameter, DHCP, or equivalent protocol but are not further described to avoid overcomplicating the herein disclosure.

Detailed Description Text (29):
In accordance with a preferred embodiment of the present invention, address procurement state object 202 is configured to communicate with an address procurement service component 128 (see FIG. 2), such as a DHCP server, using a DHCP protocol. This includes sending a DHCP request packet to address procurement service when requested to obtain a network address, such as an IP address, by a protocol handler or a service component such as a AAA server. Address procurement state object 202 also receives response packets from address procurement service component 128 which are then sent to the protocol handler which requested the service.

Other Reference Publication (1):
Ascend Communications, Inc., "Remote Access Network Security", printed from http://www.ascend.com/1103.html, on Jul. 24, 1998, pp. 1-8.

CLAIMS:

1. A method of responding to network access requests which may be based on more than one type of network access protocol, said method comprising the steps of:

receiving a first access request which is based on a first network protocol;

processing said first access request using a subscriber service independent of said network access protocol as a first task;

processing said first task by using a first protocol handler chosen by a state manager responsive to said first network protocol, said first protocol handler performing a first set of steps necessary for responding to said first access request, said first set of steps including at least one service request;

procuring at least one service upon request by said first protocol handler; and

granting or denying said first access request when a response to said step of procuring is received.

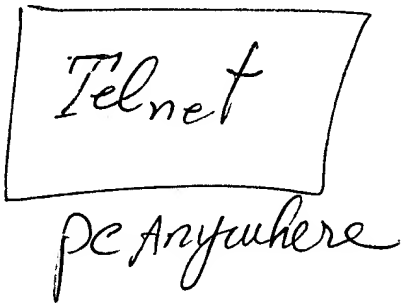
8. The method of claim 7, wherein said step of procuring a service that provides a host address includes generating a dynamic host configuration protocol (DHCP) host address request packet.

15. The method of claim 14, wherein said step of obtaining a service that provides a user record service includes generating a lightweight directory access protocol (LDAP) request packet.

For remote access, GoToMyPC is far out

Fortune; New York; Apr 2, 2001; Peter H Lewis;

Volume: 143
Issue: 7
Start Page: 192
ISSN: 00158259
Subject Terms: Remote computing
Personal computers
Software packages
Classification Codes: **9190**: *United States*
9000: *Short article*
5240: *Software & systems*
Geographic Names: United States
US



Abstract:
GoToMyPC is a secure and effective Web-based service that allows travelers to gain full access to and control over their remote computers from any browser-equipped PC anywhere in the world. The catch is that the host PC has to be powered up all the time and have an always-on Internet connection.

Full Text:

PERSONAL

TECHNOLOGY

travel technology

You're in the boondocks on business, and you've forgotten some important documents you need for the meeting tomorrow morning. No problem. Your hotel room has a broadband connection-as many do these days, even in the boonies-- and you installed GoToMyPC on your office PC before you left.

GoToMyPC is a secure and effective Web-based service that allows travelers to gain full access to and control over their remote computers from any browser-equipped PC anywhere in the world. The catch is that the host PC-the one you want to gain access to remotely-has to be powered up all the time and have an always-on Internet connection. For home PCs this means a cable or DSL connection; for office PCs, a constant LAN connection. With these connections, you can operate the PC from any distance as if you were sitting in front of it. The cursor control is a bit sluggish even over a broadband connection, but you can easily grab a file, for example, attach it to a new e-mail message, and send it off.

GoToMyPC, in free public beta testing until May 1, works only with Windows PCs for now, but Mac OS and Linux versions are expected soon. The service should cost $15 to $20 a month when it launches in May.

You can download the software from www.gotomypc.com. Expert-- city, the company that makes GoToMyPC, uses 128-bit end-to-end encryption plus multiple password challenges. Unlike other remote-- access PC systems, like Symantec's pcAnywhere or my corporate VPN (virtual private network), GoToMyPC never forced me to fiddle with port settings, IP addresses, or any other technical arcana. It even works behind corporate firewalls.

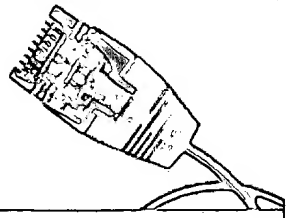
---

symantec.

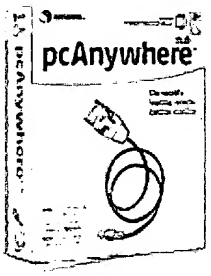
home & home office

united states
global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback

pcAnywhere 11.0™



product info reviews support buy now
Select a Product



Buy Now!

Upgrade

The world's leading remote control solution*

Symantec pcAnywhere™ 11.0 is the world's leading remote control solution.* Its integrated tools make it easy for helpdesk personnel to resolve server and workstation problems. Robust security prevents unauthorized access to enterprise resources. File transfer users will appreciate the ability to queue multiple files and then work uninterrupted while the files are transferring.

USB and DirectParallel Cable Availability

Key Features

- Solve helpdesk and server problems quickly
- Connect to remote computers securely
- Work uninterrupted while files transfer

More Details

Specifications

Current Version: 11.0

Platforms: XP Home/XP Pro/2000/NT 4/Me/98

System Requirements

Related Products

- Norton Internet Security 2003 Professional Edition
- Norton SystemWorks 2003 Professional Edition

How safe are you on the Internet?

Use Symantec Security Check to assess the vulnerability of your PC.

Award-Winning Support

For free online support 24 hours a day, visit our award-winning Web site at www.symantec.com/techsupp. Telephone support options are available for an additional fee.

Spam Watch Response Center

Resources for Symantec customers against suspicious email offers.

* Top-selling remote access software product from August 1999 through April 2003 based on The NPD Group's retail Top Selling Business Software list.

L14: Entry 6 of 13 File: USPT Jan 30, 2001

DOCUMENT-IDENTIFIER: US 6182129 B1
TITLE: Apparatus, methods and computer program products for managing sessions with host-based application using session vectors

Abstract Text (1):
Access to a session between a remote computer and an application resident at a host computer connected to the remote computer is provided via a link object embedded in a Web page accessible at the remote computer. A session is established between the remote computer and the application, and a link object associated with the established session is embedded in the Web page in response to establishment of the session. In response to termination of a session, the link object associated with the terminated session is removed from the Web page. According to another aspect, user selection of the link object associated with the established session is accepted at the remote computer. In response, a user interface to the established session, e.g., an input/output "screen," is provided at the remote computer. According to another aspect, a host access web page is accessed to establish a session. A Web page is accessed from the remote computer, and a Java applet downloaded to the remote computer in response to accessing of the Web page. The Java applet is then processed, either automatically or upon a user input, to establish a session between the remote computer. The Java applet may also be processed to embed a link object associated with the established session in the Web page. According to yet another aspect, a Session Vector is maintained which identifies sessions between the remote computer and the application. A link to a session identified in the Session Vector is maintained in a Web page accessible to the remote computer. In response to establishment of a session between the remote computer and the application, an identifier for the established session is added to the Session Vector. If a session limit has been achieved, establishment of a session may be prevented.

Brief Summary Text (9):
Conventional approaches for providing such access typically use conversion/translation techniques that employ emulation software resident at an intermediate Web server. Additional code typically executes on top of the emulation software that is capable of establishing a session from the intermediate server to a host and converting emulation screen output/input into a format understood by the browser, such as HTML files, Java GUI applets, or ActiveX controls. The intermediate code typically employs a private protocol to control the exchange of data between the server and browser in the converted format.

Detailed Description Text (12):
FIG. 2 provides an illustration of a system for managing sessions between and remote computer 110 and an application resident on a host computer 140, here shown as a 3270 application 240. The remote computer 110 may be configured to produce a platform-independent common environment, for example, a Java environment 216 (or, in Java nomenclature, a Java Virtual Machine). A Java applet 232 is stored on a server 130 at a resource location, for example, a Web page 230. The Java applet 232 may be downloaded to the remote computer 110 to be processed under the Java environment 216 to establish a session between the remote computer 110 and the application 240 on the host computer 140. For example, processing of the downloaded Java applet 218 may cause the remote computer to establish a user interface for the application, as well as control communications between the remote computer 110 and the application 240 according to the protocol required by the application 240, e.g., a TN3270 protocol.

Those skilled in the art will appreciate that although FIG. 2 illustrates a direct connection between the remote computer 110 and the host computer 140, communications therebetween may occur through one or more intermediate devices. For example, a Java security framework may require connection of the remote computer 110 and the host computer 140 through a server.

L14: Entry 3 of 13 File: USPT Feb 19, 2002

DOCUMENT-IDENTIFIER: US 6349289 B1
TITLE: Method and system for tracking computer system usage through a remote access security device

Abstract Text (1):
A system and method for monitoring remote computer access and associated costs is provided. The system includes a remotely located communication server in communication with multiple host computer networks and in communication with a network access server. First and second memory devices contain a list of authorized users for the host computer networks and a user log for use by a billing computer to generate bills. The method includes the steps of creating starting and ending time stamps for each authorized user accessing a respective one of the multiple host computer networks and creating a user log to generate bills and monitor host computer network usage.

Brief Summary Text (3):
Many organizations, both in government and in private industry, rely on access to centralized computer facilities. Use of remote access capabilities to centralized computer facilities is generally desirable in order to facilitate use of computer resources and improve productivity. Remotely located individuals who are, for example, traveling on business, often need to access their organization's computer. A concern of many organizations is monitoring the costs of remote users accessing the host computer or computer network of the company, in addition to tracking the usage of computer time and various costs associated with that time.

Detailed Description Text (2):
An advantage of the present invention is consolidation of usage and billing information in a single report. Another advantage of the present invention is the ability to manipulate the usage and billing data for each of a number of different host computer networks by individual user and by predetermined groups or departments of users at each organization. The preferred method and system cooperate with a system for securing access between remotely located computer users and the computers of different organizations for which they are permitted access.

Detailed Description Text (3):
FIG. 1 illustrates a preferred system 10 for securing access between remotely located computer users and computers of different organizations in addition to monitoring access and maintaining billing records for each host computer system. The system 10 includes at least one remotely located user computer 12. A secure identification card 14 is associated with the user and the user computer 12. A user computer 12 preferably communicates over standard telephone lines, also known as plain old telephone service (POTS) lines 17, via modem 16 through the public switched telephone network (PSTN) 18. The system 10 of the present invention may use other commonly available communication devices, such as an ISDN terminal adapter or a communications server, in place of the analog modem. The user computer may be a personal computer or another computer network. One suitable secure ID card is available from Security Dynamics, Inc. of Cambridge, Mass. and includes a display showing a time variant pass code for use by an authorized user in accessing a host computer network.

Detailed Description Text (4):
A communications server 20, which may be a router such as a Cisco 5200, is in

communication with a security service bureau 22 over a frame relay network 18. The security service bureau 22 may be a local area network (LAN) 26 that includes at least one administrative workstation 28 for monitoring operation of the security service bureau 22. A suitable administrative workstation 28 may be any of a number of commonly available personal computers. A network access server (NAS) 30 is also connected to the LAN 26. The LAN 26 of the service bureau 22 connects to the frame relay network 24 via a firewall 32. The firewall may be a personal computer, such as those available from SUN Microsystems, running software available from SOLARIS to provide protection to the service bureau LAN 26 from outside corruption. The NAS 30 may be any of a number of servers available from Hewlett Packard, such as the HP712, HP755, or the HP720. The NAS 30 of the service bureau 22 controls access of remote users, through the communication server 20 and frame relay network 24, to the multiple host computer networks 34 or stand alone computers. In the example of FIG. 1, each of the host computer networks or stand alone computers utilize the service bureau to authenticate remote users at various computers 12. One system and method for authenticating users through a service bureau is disclosed in a commonly assigned, related application identified as Attorney Docket No. 8285/141. That application is filed on the same date as the present application and is hereby incorporated by reference in its entirety.

Detailed Description Text (7):
A network management center (NMC) 39 is in communication with the ISC 35 and a private corporate intranet 19 via the ESS 37. The NMC 39 receives help requests from the ISC and provides a help desk for network infrastructure problems, performance issues and chronic desktop problems. The NMC 39 uses a pre-entered user definition and information to create a trouble record for resolving issues associated with remote access services provided to the host computer networks 34. Each trouble call is stored at the NMC 39. The NMC serves to provide proactive surveillance of all physical lines and communications servers in the system as well as handling trouble calls passed on from the ISC.

Detailed Description Text (8):
A customer service center (CSC) 40 is also linked to the system 10 via the ESS and the private corporate intranet 19. The CSC 40 manages the ordering of POTS services and repairs of business lines (e.g. DS1, ISDN, etc.). A billing application communicates over the corporate intranet 19, via the ESS 37, with the NAS 30 and other system 10 components obtain necessary billing information concerning host computer networks 34 and their respective users. Preferably, the billing application is a software application running within the ESS containing logic necessary to organize cost data by per user and per entity within a particular client's (host computers) organization. Alternatively, the billing application may be a discrete billing computer 42 executing the necessary logic to obtain and manipulate billing information.

Detailed Description Text (9):
Utilizing the system 10 described above, a preferred method of monitoring access to each of the host computer networks subscribing to the system security services is illustrated in FIG. 2. Each computer network 34 provides an associated list of authorized users that is maintained at the ISC, ESS, and NAS 30 (at step 50). An authorized user accessing a host computer exchanges the information with the NAS 30, via the communication server, each time the user dials in to gain access to his respective host computer network 34. A starting time stamp is created at the beginning of each remote access call received from a user at the communication server 20 (at step 52). In a preferred embodiment, the remote user accesses his respective host computer network by dialing in through the PSTN 18 using a modem 16 or other communication device to reach a network communications server 20. The communication server 20 forwards information on the call through the frame relay network 24 to the service bureau 22. At the service bureau 22, the NAS 30 authenticates the user through the exchange of a user name and a pass code.

Detailed Description Text (10):
The pass code preferably consists of a fixed personal identification number and a time variable security token. The security token may be a soft token, such as a software application on each authorized user's computer, or a hard token, such as a secure ID card 14 available from Security Dynamics, Inc. Each authorized user

preferably has her own security token and the security token may be a sequence of numbers, letters, or other type of symbol. Using the secure ID card 14, the security token is obtained by the user from a display that generates a new security token at predetermined time increments. The NAS 30, containing an identical security token generating algorithm synchronized with the secure ID card 14 generates the same security token to verify that the user is an authorized user. On authentication, the communication server 20 connects the user computer 12 to the appropriate host computer 34 for the duration of the call. The NAS 30 receives an ending time stamp from the communication server 20 at the conclusion of the remote access call when the user hangs up or otherwise disconnects from the host computer network 34 (at step 54). Following the conclusion of the remote access call, the service bureau stores the starting and ending time stamps in the NAS memory. Preferably the starting and ending time stamps are associated in the user log with the list of authorized users so that the user log contains a record of computer time usage for each authorized user (at step 56).

Detailed Description Text (12):
As part of the process of developing a periodic bill for customers subscribing to the system, a long distance carrier invoice is electronically transmitted to the billing computer from a long distance telephone service provider. The long distance service provider may be any one of a number of available service providers, such as Ameritech, selected by the host computer network. The long distance telephone service provider transmits a minutes of use invoice for the long distance access number used by authorized users of a given host computer network to access the security service bureau. The long distance access number may be an "800" number or other telephone number dedicated for use by authorized users to communicate with the appropriate host computer through the system 10.

Detailed Description Text (14):
Using all the information gathered, the billing computer based on the subscribed for services and the usage of each individual authorized user, various usage information and billing forms will be created. For example, in one preferred embodiment a bill may be generated that breaks up authorized users into the various departments to which they are assigned within a customer's organization. For each authorized user in the department a predetermined group of information may be displayed. This information may include per seat charges, the cost of long distance telephone usage (distributed among authorized users based on the amount of time a user was communicating with the host computer network), any equipment charges, maintenance charges, and miscellaneous charges. The per seat charges refer to fixed service charges associated with supporting each authorized user. The miscellaneous costs may include incidental security cost such as replacing secure ID cards, or for particular pieces of software necessary for enabling remote users to access their host network through the security service bureau 22. Optionally included in the per seat charges are the local exchange and other incidental charges. Once the billing summary has been generated, the billing computer can transmit the billing summary directly to the appropriate host computer network. The transmission may be done via e-mail over an internet connection, via facsimile, or through other means.

Detailed Description Text (15):
Another aspect of the presently preferred invention is that computer usage information may be provided to the customer and the service provider maintaining the security service bureau 22 so that computer resources may be optimized for usage patterns. For example, the billing computer may generate monthly or annual reports dividing up the usage for each individual authorized user by total time used per a given period or by time of day or week so that host computer network 34 or service bureau 22 resources can be properly allocated for particularly heavy usage.

Detailed Description Text (16):
From the above, a new system and method of monitoring access and fees for host computer networks with relocated users is provided. The method includes maintaining a list of host computer networks and associated list of authorized users for each network, creating a starting and ending time stamp for remote access calls, transmitting the starting and ending time stamps in the user log to a billing computer in addition to other billing information, and generating a billing summary of costs and usage at the billing computer. The system preferably includes a

security service bureau providing secure remote access between remotely located authorized users and their respective proprietary host networks. In one preferred embodiment, the NAS preferably records time stamps and a user log indicating usage of resources by individual authorized users. A billing computer is also included in the system having the logic necessary to compile information from the user log in the security service bureau and cost information received from outside sources to generate a periodic bill indicating cost per individual user and/or department.

CLAIMS:

1. In a system for providing secure remote access between a plurality of unrelated host computer networks and a plurality of authorized users via a network access server, a method of monitoring access to each of the unrelated host computer networks comprising the steps of:

maintaining a list of host computer networks and an associated list of authorized users for each host computer network in a first memory device;

automatically creating a starting time stamp at the beginning of a remote access call received from an authorized user at a communication server and connecting the authorized user to an appropriate one of the plurality of unrelated host computer networks after determining at the network access server that the authorized user is authorized to connect to the appropriate one of the plurality of unrelated host computer networks;

automatically creating an ending time stamp at a conclusion of the remote access call;

storing the starting and ending time stamps for the remote access call in a user log in the network access server, the starting and ending time stamps associated with the list of authorized users whereby the user log contains a record of computer time usage for each authorized user;

transmitting the user log from the network access server to a billing computer;

transmitting the list of host computer networks and the associated list of authorized users for each host computer network from the first memory device to the billing computer; and

generating a billing summary at the billing computer for each of the host computer networks.

12. In a system for providing secure remote access between a plurality of unrelated host computer networks and a plurality of authorized users via a network access server, a method of monitoring access to each of the unrelated host computer networks comprising the steps of:

maintaining a list of host computer networks and an associated list of authorized users for each host computer network in a first memory device;

receiving a remote access telephone call to a host computer network from a user computer of an authorized user at a communication server;

automatically creating a starting time stamp at the beginning of the remote access call received from an authorized user at the communication server and connecting the authorized user to an appropriate one of the plurality of unrelated host computer networks after determining at the network access server that the authorized user is authorized to connect to the appropriate one of the plurality of unrelated host computer networks;

automatically creating an ending time stamp when the user computer terminates the remote access call with the host computer;

storing the starting and ending time stamps for the remote access call in a user log in the network access server, the starting and ending time stamps associated with

the list of authorized users whereby the user log contains a record of computer time usage for each authorized user;

transmitting the user log from the network access server to a billing computer;

transmitting the list of host computer networks and the associated list of authorized users for each host computer network from the first memory device to the billing computer; and

generating a billing summary at the billing computer for each of the host computer networks.

13. The method of claim 12, wherein connecting the authorized user to an appropriate one of the plurality of unrelated host computer networks after authenticating comprises communicating with a security server to authenticate that the authorized user may access a host computer network and connecting the authorized user to the host computer network via the communication server.

WEST

Generate Collection Print

L8: Entry 4 of 6 File: USPT May 28, 2002

DOCUMENT-IDENTIFIER: US 6397254 B1
TITLE: Access-method-independent exchange 3

Brief Summary Text (5):
The term "The Information Superhighway" is commonly thought of as an extension of the Internet, a network linking hundreds of thousands of computer systems together and communicating via a standard protocol.

Brief Summary Text (7):
As computer networks have developed, various approaches have been used in the choice of communication medium, network topology, message format, protocols for channel access, and so forth. Some of these approaches have emerged as de facto standards, but there is still no single standard for network communication. The Internet is a continually evolving collection of networks, including Arpanet, NSFnet, regional networks such as NYsernet, local networks at a number of university and research institutions, a number of military networks, and increasing, various commercial networks. The protocols generally referred to as TCP/IP were originally developed for use through Arpanet and have subsequently become widely used in the industry. The protocols provide a set of services that permit users to communicate with each other across the entire Internet.

Brief Summary Text (10):
The Internet Protocol (IP) is implemented in the third layer of the OSI reference model, the "network layer," and provides a basic service to TCP: delivering datagrams to their destinations. TCP simply hands IP a datagram with an intended destination; IP is unaware of any relationship between successive datagrams, and merely handles routing of each datagram to its destination. If the destination is a station connected to a different LAN, the IP makes use of routers to forward the message.

Brief Summary Text (13):
As shown in FIG. 10, the OSI model provides for three layers above the transport layer, namely a "session layer," a "presentation layer," and an "application layer," but in the Internet these theoretical "layers" are undifferentiated and generally are all handled by application software. The present invention provides for session control and for communicating with applications programs. Thus the present invention may be described in accordance with the OSI theoretical model as operating at the session layer and application layers.

Brief Summary Text (54):
There are several modifications permitted. First, when a communication point is registered, the registering process can identify the communication point as a public point. As such, only one instance of the service needs to be executing at any time. All processes requesting to use this point will share the same primitive. Alternatively, a service can be registered as a private service, in which case each process requesting communication to the service will be connected to their own instance of the service. Finally, when a service is initially registered, a maximum number of connection points can be preset. When this limit is reached, then all new processes requesting access to the service will be denied, until such time as the number of current instantiations of the service falls below the threshold.

Brief Summary Text (66):

Using TCS for Remote Communication

Brief Summary Text (86):
13. Token describing if a private connection to the service can be used

Brief Summary Text (88):
15. Token describing if a private connection is mandatory

Brief Summary Text (95):
22. Series of status information components including but not limited to security privileges and owner information.

Detailed Description Text (13):
Alternatively, when using a graphical user interface with an Icon, the name of the Application Program, its specific location on the computer system, and other information is required to execute the Thread. A further limitation of the Icon is that one Application Process can be started by selecting the Icon, but that Application Process cannot select a new Icon to execute as an Application Co-Process. That is to say, the Icon is a graphical representation for the end user to select.

Detailed Description Text (64):
In registering a new service, a series of attributes are provided by the registering thread describing the type of service to be provided. These attributes are classified as Public or Private attributes. Public attributes are considered public information and are accessible through the Thread Directory Service by any thread executing locally, or remotely. Private attributes are only accessible by the Thread Directory Service. The administrator of the Thread Directory Service has access to all attributes. A complete description of the attributes is provided in the Embodiment section below.

Detailed Description Text (241):
13. token describing if a private connection to the service can be used;

Detailed Description Text (243):
15. token describing if a private connection is mandatory;

Detailed Description Text (250):
22. series of status information components including but not limited to security privileges and owner information;

Detailed Description Text (638):
PRIVATE: a private version of the AMS must be executed.

Detailed Description Text (659):
The CAMS will allocate a storage area, referred to as the MAP AREA for the specified AMS and associate an identifier with this MAP AREA. The CAMS will mark the MAP AREA with administrative information including, but not limited to the specific machine architecture on which the specified AMS is currently executing, timing information, security information to prevent unauthorized access to the MAP AREA, ownership information indicating the specified AMS as the owner of this MAP AREA and other information.

Detailed Description Text (714):
6. Attributes describing security requirements

Detailed Description Text (725):
The entries in the NEECF may include specifications identifying remote computer system accessible to the current computer system through some form of communications mechanism. Such an entry includes information detailing if the remote computer system is expected to have a NEEM executing on it, and/or, if there is a NEECF located on that computer system.

Detailed Description Text (731):
an attribute describing if the NEE is PUBLIC or PRIVATE

WEST

Generate Collection Print

(1)

301

L5: Entry 2 of 3 File: USPT Jul 26, 1994

DOCUMENT-IDENTIFIER: US 5333152 A
TITLE: Electronic mail remote data transfer system

Abstract Text (1):
An apparatus connecting and establishing a communication link between a local and a remote computer to provide transfer of data wherein the remote computer is activated by a control unit, identification and protocol established and data transferred, as may be applied to provide personal electronic mail service. The preferred embodiment interposes the control unit between a non-dedicated telephone line and a remotely located personal computer having a modem therein, wherein a computer power-switching relay is connected to the control unit and is energized upon recognition of a selected protocol as provided by selected program control of the originating computer, and the communications link established via program responses of the remote computer and programmed signal initialization and responses of both computers according to firmware in the controller. Thus, according to the present invention mail transfers to or from an unattended remotely controlled computer is provided by activating an unattended remote computer or interruption of ongoing remote computer operations, such as word processing at the remote computer. Furthermore, according to the present invention, two levels of access security are provided by the control unit without further encumbering the sequence and process of data transfer.

Brief Summary Text (2):
The present invention relates to data transfer systems, in particular, data transfer systems providing file transfer between a local and an attended or unattended remote computer via telephone line or other communication medium.

Brief Summary Text (4):
Data transfer to or from remote data equipment such as home personal computers has heretofore required the presence of an operator to power-up and initialize the remotely located computer in preparation for receiving or transmitting data. If unattended, such remotely located computers would necessarily be left on and preset to receive file transfer commands or other instructions to provide the desired data transfer. Such continuous operation, however, results in continuous power consumption, increased component wear, and makes the remote unit vulnerable to sophisticated intrusion efforts wherein data may be lost, damaged or unauthorized access gained. In an attempt to reduce power consumption and component wear, some systems include a power switch which is responsive to telephone line ringing signals wherein the personal computer is normally off except after an incoming telephone ring (referred to as a "ring-forward") signal is detected. Thereafter, the computer is turned on and configured to answer the ringing signal. However, such systems provide no pre-screening of non-data or unauthorized calls, resulting in needless sequencing of the computers whenever a telephone call is received. Furthermore, some modems answer immediately after receiving power and will therefore answer the ring-forward signal before essential communications software becomes active following boot up. Alternately, such remote systems require dedicated telephone lines, not normally provided or economically justifiable in the typical home or small office computer environment. Additionally, if a remote computer system is connected to a non-dedicated telephone line, no prioritized allocation of the line among a plurality of telephone line-associated equipment, such as a telephone desk set, an automatic answering machine, and the local personal computer is provided.

Brief Summary Text (6):

The system and apparatus according to the present invention automatically establishes a data transfer path between local data equipment and remotely located data equipment over a non-dedicated telephone line shared by other telephone apparatus such as a desk set and an automatic answering machine. According to the present invention, the remotely located data equipment is supervised by a control unit which provides the above-mentioned access security, energizing the computer only upon successful entry through the security check, thereby minimizing the power cycling of the remotely located data equipment due to other uses of the telephone line and unauthorized attempts at system entry. Moreover, the control unit included in the system according to the present invention will provide for the shared connection of an automatic call answering device, such as a voice answering machine to the telephone line, wherein upon detection of selected dual-tone multi-frequency (DTMF), or "touch-tone" (TM), password signals on the telephone line, the control unit will disconnect the automatic answering device, apply power to the data equipment if necessary, generate a ring signal voltage capable of causing the data equipment modem to respond as though connected directly to the telephone line, provide subsequent alphanumeric security code processing and, if successful, the ultimate data file transfer. Furthermore, according to the present invention, the local data terminal and the remote data terminal, both typically comprising personal computers, are programmed to automatically establish the file data transfer capacity, as may be applied to electronic mail applications, and include a level of alphanumeric password security inhibiting unauthorized access to the remotely located data files. A further feature of the present invention allows the status of the remotely located data system or the control unit itself to be determined at any available telephone having touch-tone signalling wherein a predetermined touch-tone code sequence results in an audible response from the control unit indicating the requested status such as data system power-on or power-off.

Brief Summary Text (7):
Moreover, if the remote computer system is currently engaged in an activity, as may be provided in any one of several operating systems, such as word processing, the system according to the present invention will minimally interrupt the ongoing operation of the remote computer to provide the data transfer, in the worst case, suspending the current operation to accomplish the data transfer and returning immediately thereafter to the point of operation prior to data transfer. Therefore according to the present invention, a system is provided wherein electronic mail service can be provided to a minimally configured remote location having non-dedicated telephone lines which decouples the incoming ring, boot up, and the local ring events so as to accommodate the timing needs of any PC installation.

Drawing Description Text (3):
FIG. 1 is a block diagram of a system including the remotely located computer and the control unit according to one embodiment of the present invention;

Drawing Description Text (7):
FIG. 4 is a flow chart showing the program resident in the remotely located computer according to FIG. 1;

Detailed Description Text (2):
The present invention is shown in FIG. 1, in a system 50 which provides the file transfer between a local computer 52 and a remote computer 54 through a communication medium such as a telephone line 56 through modems 53 and 55 in, or connected to, computers 52 and 54 respectively. According to the present invention, control of the remote computer 54 is provided by a control unit 58 which is connected to a non-dedicated telephone line 56. The non-dedicated telephone line can also be connected to other devices such as a desk set 57 and an answering machine 51. Power to the remote computer 54 is controlled by the power unit 59 connected to the control unit 58. The local computer 52 and the remote computer 54 include operating system software such as MS-DOS (TM) and may be further programmed with software such as LOTUS 1-2-3 (TM). The local computer 52 is operable according to a program comprising this invention as illustrated by the flow chart of FIG. 3, to originate the establishment of data or file transfer. The remote computer 54 is operable by program software comprising this invention as illustrated by the flow chart of FIG. 4 to provide a response to a request for data transfer. The remote computer control unit 58 comprises the hardware illustrated in FIGS. 2A and 2B and

is operable according to the flow charts of FIGS. 5-12, as well as modifications made by those of ordinary skill in the art.

Detailed Description Text (3):
According to one embodiment of the present invention, both the local computer 52 and the remote computer 54 and their respective modems 53 and 55 are commonly available commercial products such as the IBM PC computers and the Hayes modems or their equivalent. The modems may be internal components of the computers or connected externally. The communication medium 56 typically comprises a normal telephone line 56, but other media may be used, for example isolated wiring employing the standard RJ-11 telephone jacks may be used in the home. The telephone switching office operates conventionally and forms no part of the invention. Similarly, the telephones 57 and 57A illustrated in FIG. 1 and the answering machine 51 comprise standard commercially-available units. Therefore, the present invention permits the above-mentioned and below-described improvements with minimal interference with standard system configurations, except for the redirected telephone line connections through the control unit 58 and the power connection through the power unit 59.

Detailed Description Text (4):
The control unit 58 of FIG. 1 is described in greater detail by the schematic diagrams illustrated in FIGS. 2A and 2B and the flow chart illustrations of the firmware stored in the memory 152 and executed by the microprocessor 150, according to the flow chart representations of FIGS. 5-12. In the schematic diagram 60 of FIG. 2A, a telephone line 56 of FIG. 1 is connected to line-in jack 102 which provides connection to telephone 57 through local phone jack 104 and connection to relays 106 and 108. In a quiescent or power-off condition, the relays 106 and 108 provide connection of an auto answering device, such as a telephone answering machine and a facsimile machine, via jack 110 to the line input 102 for normal automatic answering. Relays 106 and 108, controlled by their respective transistors and microprocessor 150 of FIG. 2B route the telephone signal as described previously, and in greater detail below. For instance, when touch-tone or data signals are detected, such as by the DTMF receiver 112 of various manufacturers, which is connected to receive signals from the line input from jack 102, by the microprocessor 150 connected to receive the four digital signals from the DTMF receiver 112, they cause the relay 108 to become energized, disconnecting the answering device connected at jack 110 and connecting the modem of the remote computer 54 or other telephone device connected via jack 114. Simultaneously, the microprocessor 150 of FIG. 2B enables the power unit 59 of FIG. 1 to power the remote computer 54 via pins 28-31 of the microprocessor 150. Having turned on the remote computer 54, the associated modem 55 is now operable to receive signals, whereupon the microprocessor 150 generates a 20 Hz high-voltage ring signal via circuit 120 which is applied to the modem by relay 106 as controlled by the microprocessor 150 through the transistor associated with relay 106 and provide a ring-back signal to said signal line input.

Detailed Description Text (8):
According to the present invention, the local computer 52 of FIG. 1 includes a program which operates in the context of an operating system, such as the one belonging to the Apple Macintosh, or DOS in the case of IBM PC-type computers. The program, although not necessary for some aspects of the present invention, provides for the automatic origination of data file transfers as illustrated in the flow chart 80 of FIG. 3. The destination telephone number is dialed at step 202 and a DTMF password is repetitively sent at step 204. After transmission of the DTMF password at step 204, the local computer waits for a signal tone relayed by the control unit 58 at step 206, until a specified time, such as 120 seconds, has elapsed, as provided by step 208. If a carrier is detected, as provided by the remote computer control unit 58, the local computer then supplies the caller identification (ID) and password at step 210 when prompted by the remote computer 54 at step 242 of FIG. 4. A typical correct response results in a successful log-in process at step 212, which is then followed by the transfer 214 of the data between the remote computer 54 and the local computer 52. The results of the file transfer are reported at 216, typically by an on-screen or other visual or audible indication as may be provided. Specifically, the receipt of a file results in a flashing indicator light and the appearance of an on-screen indicator. Similarly, if more than the specified time has elapsed, a failure to connect is reported at step 218

and a log-in failure, such as the refusal of the log-in caller ID and/or password is reported at step 220.

Detailed Description Text (9):
The remote computer 54 includes a program which responds to the telephone-ringing flags set by the modem 55 when the remote computer 54 is powered-on by the power unit 59 in response to the control unit 58, which was in turn previously activated by the signal sequence discussed above as iterated by the local computer 52. The program sequence is described generally in flow chart 82 of FIG. 4, wherein the remote computer 54 optionally loads and executes the service program of 82 at step 230, and begins polling the modem to determine if a telephone ringing signal is being received at step 232. If a ringing signal is detected by the modem, the cadence of the signal, meaning the characteristic durations of AC ring voltage present and absent in a cycle, is examined at 233. If the cadence is recognized as that generated by the control unit 58 to indicate that an automatic data transfer is desired, the modem is commanded to answer (go off-hook) at step 234 and wait for a carrier detect within a specified time period, e.g. 120 seconds, steps 236 and 238. If instead a determination is made at step 233 that the cadence indicates a different communications program is desired, this program, identified earlier during installation of software on the remote computer 54, is executed at 235. Step 233 thus permits more complete access to the files on the remote computer 54, afforded by the more elaborate program 235, at the cost of consuming more of the computers resources and effectively preempting simultaneous operations under the DOS operating system. If no carrier is detected at step 238 the modem is reset at step 240 and the remote computer 54 again awaits the ringing signal at step 232. If a carrier is detected at 236, a signal is sent to the local computer 52 which requests or prompts the local computer 52 to provide a caller ID and a password at step 242. The caller ID and password are verified at step 244, and if found appropriate a file transfer is executed at step 246. If at least one of the received caller ID and password fails to belong to the set of valid caller ID and password combinations stored at the remote computer 54, the modem is reset at step 240. The transfer of a file or other data at step 246 is completed after which the transfer is reported by appending an entry to an event log file and issuing an on-screen or audible operator signal at step 248.

Detailed Description Text (10):
The control unit 58 associated with the remote computer 54 includes a microprocessor-controlled system having firmware to provide the appropriate detection, signalling, and control functions. The main processing loop flow chart 84 is shown in FIG. 5. Upon initial power-up, such as when first plugged into the power mains of the remote site, the control unit provides an automatic power-up self-test at step 260. All internal and external signals are reset at step 262 and the main program enters a loop. The main loop includes a test 264 to determine if a telephone line ringing condition exists. If a ringing signal is present on the telephone line 56 connected at jack 102, the line ringing subroutine 86 of FIG. 6 is begun. An off-hook condition of the line is determined at step 266, and the line off-hook subroutine 92 of FIG. 9 is entered. If the modem 55 of the remote computer 54 is off-hook, as determined by step 268 via sub-circuit 148 of FIG. 2A, the modem off-hook subroutine 94 at FIG. 10 is begun. If the "ready" button 121 (FIG. 2A) is depressed (contact closed), as determined by step 270, the ready-button-down subroutine 96 of FIG. 11 is begun. If the "PC power" button 119 (FIG. 2A) used to manually turn on the remote computer is depressed, the power-button-down subroutine 98 of FIG. 12 is begun. Until one of the above conditions is detected, the main processing loop 84 repeats. Upon completion of any of the aforementioned five tests and related subroutines, the programs re-enter the main processing loop prior to step 262, wherein the control unit signals are reset.

Detailed Description Text (12):
The automatic-mode DTMF password subroutine 88 of FIG. 7 identifies one of at least two local ring signal cadences, step 303, and one of at least two "ready" LED flash modes, step 305, associated with the automatic-mode DTMF password recognized at step 290, that will govern control unit actions for the modem or other telephone device 114 as well as disconnect any present automatic answering device 110. A determination is made whether the power of the remote computer 54, via power unit 59 is on at step 302. If not, the computer power is turned on and a ringing limit (e.g.

12 times), discussed below, is set in step 304. If the power to the computer 54 is currently on, a smaller ring limit (e.g. 8 times) is set in step 306. Next, at step 308 a ringing signal to the modem 55 is generated (120, FIG. 2A). The processor 150 fixes the frequency of the local ringing signal through firmware timing loops, and synchronously gates current pulses to the "modem in use" indicator so that the indicator flashes with the same frequency (e.g. 20 Hz in the preferred embodiment). If the modem has answered, step 310 (under control of the receive file transfer program 82, step 234), the ringing signal is cancelled at step 312, and a line on-hook test is made, step 314 to determine if the modem is on-hook. If the line is on-hook (140, FIG. 2A), signaling the completion of the file transfer and the disconnect of the call, the "ready" LED indicator is caused to flash, step 316 according to the flash mode identified in step 305. The flash mode associated with a selected password may correspond to a flash rate or even cause the indicator to stay on continuously, i.e., not flash. In this way certain data transfer operations which do not require attention at the remote computer such as files transferred from, rather than to, the remote computer, will not trigger the flashing indicator. At step 311, a determination is made whether the remote computer 54 power was on at the time the automatic-mode DTMF password was recognized. If the power was not on, meaning that it was turned on at step 304 for the purpose of servicing the current call, step 309 provides for the removal of power from the remote computer 54 after a selected time interval, nominally 10 seconds. According to the present invention, the processor 150 is programmed to provide flashing the "PC power" LED with a duty cycle proportional to the imminence of this automatic power removal. Over the defined time interval, the "PC power" LED indicates that a pending power-off situation exists by drifting from a "mostly on" appearance to a "mostly off" appearance before turning completely off coincident with the removal of power from the remote computer 54. This time interval may last ten seconds, ten minutes, as desired. The system then returns to the main processing loop before step 262. If the modem has not answered, step 310 and the ring limit (nominally 8 or 12) has been reached at step 318, and the current ring sequence was not the first attempt, step 320, the "ready" LED indicator is turned off, step 322 and the system resumes the main processing loop before step 262. On the first attempted ring sequence in which the ring limit is reached, as determined at step 320, the computer 54 power is turned off for four seconds and then again turned on, and the ring limit is set to 12 at step 324; the sequence is begun again at step 308 wherein the modem ring signal is provided.

Detailed Description Text (13):
Moreover, general mail may be received at step 246 according to the present invention when universal (not selected) DTMF and alphanumeric passwords are detected at steps 290 and 244, respectively. The universal DTMF password, identical for all installations of the present invention, is one of at least two automatic-mode DTMF passwords that the control unit 58 is capable of recognizing at step 290. Likewise, the universal alphanumeric caller ID and password are identical for all installations and are verified at step 244. The universal DTMF and alphanumeric passwords may be selectively enabled so as to accept mail from unknown callers at the remote computer 54 while maintaining selective file security to prevent unauthorized access to computer 54 files. When the universal passwords are selectively disabled, no access is granted to unknown callers.

Detailed Description Text (15):
The interactive-mode DTMF password subroutine 90 of FIG. 8 responds to the detection of the interactive-mode DTMF password, step 294 of FIG. 6, whereupon a "greeting" tone sequence is sent to the initiating party and a load 113 placed on the line input to maintain an off-hook condition and relay 108 is energized so as to disconnect any device connected at jack 110, step 330. If a command has been entered at step 332 and it is determined to be valid at step 334, an "accept" tone sequence such as two notes of ascending pitch is placed on the telephone line at step 336. If a command has not been entered and more than 30 seconds have elapsed, step 334, the main processing loop is re-entered before step 262. If a command has been entered, at step 334 but is invalid, a "reject" tone sequence such as two notes of descending pitch is provided, step 340, and the 30-second command time-out interval timer is reset at step 342, prior to re-entering the command test at step 332. Once the "accept" tone sequence has been provided at step 336, the particular query of the initiating party is determined at step 344. If the query relates to the PC on/off

status which is determined at step 346, a "true" tone sequence is returned to the initiating party via the telephone line at step 348 if the power is on, and a "false" tone sequence is returned to the initiating party if the power is off, step 350. Typically, the true tone sequence comprises a reference tone followed by a higher-pitched tone, while the false tone sequence comprises the same reference tone followed by a lower-pitched tone. Upon generation of the tone sequence, the command time-out is reset at step 342. If the received command is not a state query, a test is made at step 352 whether the initiating party intends to control the power of the remote computer 54. If so, the power unit 59 is energized or de-energized according to the received command and the power LED indicator is likewise turned on or off, step 354 and the 30-second command time out, 342, is reset. If the signal received is neither a power command or a query, the system according to the present invention provides a "ring-through" command which is detected at step 356 which causes the automatic-mode DTMF password subroutine 88 of FIG. 7 to begin. If the command is neither a ring-through command nor one of the previously discussed commands, the present system provides for additional commands.

Detailed Description Text (18):
If the modem is off-hook, step 268 of FIG. 5, the modem off-hook subroutine 94 is begun, FIG. 10 wherein the modem relay 108 is energized and the line in-use and modem in-use LED indicators are turned on, step 390. The modem is tested to determine if it is on-hook at step 392, whereupon the program re-enters the main processing loop before step 262 if the modem is on-hook. If the modem is not on-hook, step 392, and the "PC power" button is down, step 394, the power status of the remote computer 54 is tested at step 396, whereupon the computer power is turned on as well as the power LED indicator at step 398. If the remote computer 54 power is on, it is turned off and the power LED indicator is turned off at step 400. Subsequently the status of the "PC power" button is detected at step 402, whereupon the modem on-hook test at step 392, is again provided, if the "PC power" button is depressed at step 394, and if the "PC power" button is not depressed at step 402.

Detailed Description Text (19):
If the "ready" button is down, as determined by step 270 of FIG. 5, the ready-button-down subroutine 96 of FIG. 11 is begun wherein the flashing of the "ready" LED is cancelled at step 410, and the status of the "ready" button is provided at step 412, whereupon the program re-enters the main processing loop before step 262 if the "ready" button is up. If the "ready" button is not up and three seconds have not elapsed, the "ready" button-up test at step 412 continues; if more than three seconds have elapsed at step 414, a ready-to-receive test is begun which comprises steps numbered 416 through 436. This sequence of operations verifies the operability of the remote computer 54, circuits of the control unit 58, modem 55, all necessary electrical connections, and program steps 230, 232, and 233 diagrammed in FIG. 4 to work in concert to successfully execute step 234 of FIG. 4. Toward this end, if the remote computer 54 power is on at step 416, the remote computer power is turned off and a four-second pause is executed, at step 418. If the remote computer 54 power is not on, it is turned on and the ring limit nominally set to 12 rings, at step 420. The modem is signalled by a ring voltage 120 at step 422. It is then determined whether the modem has answered the ring signal, step 424, whereupon the in-use LED indicators are activated and the ringing signal is cancelled at step 426 if the modem has answered the ring signal. Thereafter, it is determined if the line is on-hook, step 428, whereupon the test is continued for three seconds at step 430. If more than three seconds has elapsed and the line is not on-hook, the "ready" LED indicator is energized at step 432 and the line is tested at step 434 to determine if it is on-hook. If the line is on-hook, the original power state (on or off) is restored at step 436 and the main processing loop is re-entered before step 262. If the modem has not answered (gone off-hook), 424, and the ringing limit has been reached at step 438, the "ready" LED indicator is set to off at step 440 and the original power state is restored at step 436. If, in the main processing loop 84, i t has been determined that the "PC power" button is down, step 272, the power-button-down subroutine 98 of FIG. 12 is begun, wherein the status of the PC power is determined, step 450, and the embodiment remote computer is turned on and the power LED activated, step 452 if the remote computer 54 is not currently on. If the remote computer 54 is already on, it is turned off and the power LED indicator is deactivated, step 454. Thereafter, the status of the "PC power" button is determined, step 456 and the main processing loop 84 re-entered

before step 262 when the "PC power" button is released.

Other Reference Publication (2):
Product Brochure "PC Power Center", Power up a PC from anywhere, Anytime; EKD, Selden, N.Y.

CLAIMS:

8. Apparatus for providing remote initiation of a data transfer with a local computer via a communications line, comprising:

means for sensing a ringing signal on communication line;

means responsive to said sensed ringing signal for providing an answer condition after a selected number of rings wherein the ringing signal terminates and said communication line is in condition to transfer data thereon;

a password decoder for providing an enable signal upon receipt of a selected password comprising a first data sequence;

a local ringing signal generated for providing a local ringing signal to said local computer in response to said enable signal; and

a power switch adapted to cause said local computer to become powered in response to said enable signal, wherein

said local computer includes means responsive to said local ringing signal for providing an answer condition,

said local ringing signal generator terminates said local ringing signal, when said means responsive to said local ringing signal answers so as to provide data transfer between said local computer and said communications line.

13. A method of providing data transfer between a local computer and a remote computer, comprising the steps of:

establishing communications between said local computer and a remote computer control unit;

transmitting a selected password from said local computer to said remote computer control unit;

providing power to said remote computer upon receipt of said selected password;

providing a local ringing signal to said remote computer from said remote computer control unit;

answering said local ringing signal;

executing a selected program in said remote computer to service said communications between said local computer and said remote computer upon answer of local ringing signal;

respectively providing a selected alphanumeric ID password from said local computer after a carrier link is established and a prompt is issued by said remote computer; and

providing a transfer of data between said local computer and said remote computer.

14. The method of claim 13, wherein the step of establishing comprises

providing a telephone line connection between modem associated with said local computer and said remote computer control unit.

16. The method of claim 13, further including the step of transmitting a ringback

signal to said local computer from said remote computer control unit upon receipt of said selected password.

17. The method of claim 16, further including the step of executing a program in said local computer to provide said selected alphanumeric password in response to said prompt issued by said remote computer.

18. A method of determining the status of a remotely located computer via a communication link, comprising the steps of:

establishing communications with a remotely located computer control unit via said communications link;

signalling said remotely located computer control unit with a selected password;

signalling said remotely located computer control unit with a selected inquiry code; and

returning a status signal in response to said selected inquiry code by said remotely located computer control unit,

wherein the step of signaling comprises the step of signaling an interactive-mode password comprising on of a status and a command.

19. The method of claim 18, wherein the step of establishing comprises the step of providing a telephone connection by manually dialing the telephone number associated with said remote computer and the corresponding control unit.

20. The method of claim 18, further including the step of providing the status of one of said remote computer and said remote computer control unit.

21. The method of claim 18, further including the step of obtaining the state of one of said remote computer and said remote computer control unit.

WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Term	Documents
(4 AND 3).USPT.	3
(L4 AND L3).USPT.	3

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L5

Refine Search

Recall Text | Clear

Search History

DATE: Tuesday, July 08, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L5	L4 and l3	3	L5
L4	PC anywhere	42	L4
L3	remot$ and transfer$ file	1086	L3
L2	L1 and remote and transfer$ file	29	L2
L1	Scott.in.	22328	L1

END OF SEARCH HISTORY

L5: Entry 3 of 7 File: USPT Feb 4, 2003

DOCUMENT-IDENTIFIER: US 6516341 B2
TITLE: Electronic mail system with advertising

Brief Summary Text (16):
Advertisers find it desirable to target advertisements to relevant potential customers. For example, an advertiser of stockings would prefer to target women rather than men with its advertising. A Boston restaurant would prefer to target residents of Boston and business travelers rather than children living in San Francisco. Moreover, advertisers prefer to pay for advertising based upon the number of relevant consumers who are actually exposed to the advertisement. For prior on-line systems and networks, including the World Wide Web, it is often difficult for an advertiser to precisely determine whether its advertisements were actually viewed by a user and for how long, and whether the advertisement induced a response. Accordingly, there exists a need for a targeted advertisement system that also can provide information as to the characteristics of those who were exposed to each advertisement, for how long the user was exposed, and at what times.

Brief Summary Text (22):
In the representative embodiment of the present invention, a client computer is used by each user and runs a client program. The client computer may be, for example, a personal computer with an Intel Pentium or 486 processor and a Microsoft Windows or OS/2 operating system. The client computer has the capability to connect to a remote computer network, e.g., by modem. The client computer also has a secondary memory device, such as, for example, a hard disk drive. The client program of the present invention is stored on the hard disk drive and is executed by the client computer's processor.

Brief Summary Text (48):
Moreover, an advertisement may be downloaded once but viewed many times by a user, thus reducing transmission costs. The advertiser can be billed for the multiple viewings of the advertisement. This is in sharp contrast to advertisements displayed on the World Wide Web, where a user may visit a web site many times but because of caching functions of most web browsers, the advertiser is unaware that the advertisement has been viewed more than once. Further, web advertisers at present have no way of determining for how long the advertisement was displayed to the user. Thus, the integrated targeted advertisement system of the present invention provides a number of advantages over web-based systems. According to the present invention, users willingly identify themselves and their consumer interests, and make user verification possible. Furthermore, the system of the present invention can provide extremely accurate data as to how long an advertisement was shown to a user, when it was clicked on, and how many times it was shown before the user responded to the advertisement.

CLAIMS:

32. An e-mail system for use by a plurality of users, comprising: a server system, including means for determining additional content that is relevant for each user; means enabling the creation and reading of e-mail messages at remote computers while said remote computers are off-line with respect to the server system; means for transferring e-mail messages between said remote computers and the server system while said remote computers are on-line with respect to the server system; means for transferring relevant additional content from the server system to remote computers

while said remote computers are on-line with respect to the server system; means for storing the transferred additional content locally at the remote computers; means for outputting the stored additional content at the remote computers when e-mail messages are being created or read at the remote computers.

WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Term	Documents
(4 AND 1).USPT.	7
(L1 AND L4).USPT.	7

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: [ ] Refine Search

Recall Text | Clear

Search History

DATE: Tuesday, July 08, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=ADJ			
L7	l1 and l4	7	L7
L6	l1 and l3	1	L6
L5	L4 and l3	7	L5
L4	web based	1864	L4
L3	traveler$1 and remote computer	97	L3
L2	L1 and remote access$	14	L2
L1	Lewis.in.	8756	L1

END OF SEARCH HISTORY

WEST

Generate Collection Print

L3: Entry 2 of 25 File: USPT Apr 15, 2003

DOCUMENT-IDENTIFIER: US 6549612 B2
TITLE: Unified communication services via e-mail

Abstract Text (1):
A method and system for providing unified messages services to a subscriber. The subscriber utilizes an active interface embedded in an e-mail notification to control delivery of a non-literal, single media or multimedia message to the subscriber. Such a non-literal message includes, but is not limited to, any of a hyperlink-based message, a voicemail message, a facsimile, and a video clip. The active interface provides access to communications-related services as well, including access to stock/options trading and bill payment.

Brief Summary Text (8):
Documents are also available which describe electronic mail handling procedures. In particular, two Internet standards on e-mail are incorporated herein by reference in their entirety. They are: Internet STD014 entitled "MAIL ROUTING AND THE DOMAIN SYSTEM" (also known as RFC 974) and Internet STD0010 entitled "SIMPLE MAIL TRANSFER PROTOCOL" (also known as RFC 821). The contents of the Second Edition of "sendmail" by Bryan Costales and Eric Allman, published by O'Reilly Publishing, is also incorporated herein by reference. Additional Requests for Comments that describe mail formats that are incorporated herein by reference are: RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, November 1996; RFC 2046 Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, November 1996; RFC 2047 MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text, November 1996, RFC 2048 Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures; November 1996; and RFC 2049 Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples; November 1996.

Detailed Description Text (3):
The computer system further includes at least one computer readable medium. Examples of such computer readable media are compact discs 119, hard disks 112, floppy disks, tape, magneto-optical disks, PROMs (EPROM, EEPROM, Flash EPROM), DRAM, SRAM. Stored on any one or on a combination of the computer readable media, the present invention includes software for controlling both the hardware of the computer 100 and for enabling the computer 100 to interact with a human user. Such software may include, but is not limited to, device drivers, operating systems and user applications, such as development tools and (graphical) system monitors. Such computer readable media further include a computer program, according to the present invention, for providing unified messaging. In addition, the software includes a program or programs (including device drivers) for interacting with a remote voice messaging service, telephone switches or bridges, and/or facsimile servers. Examples of known telephone bridges are 1) the LNX 2000 by Excel and 2) the SDS-500 by Summa Four Inc. The software can control the voice messaging services and switches under the control of the Unified Communications (UC) server of the present invention based on a user's interaction with his/her "active" e-mail.

Detailed Description Text (19):
By leveraging the rendering capabilities of e-mail programs, a rich graphical HTML interface is provided when rendering an e-mail. Below is step by step analysis of one embodiment of a method of sending a subscriber notification--specifically a notification that a voicemail message is in the subscriber's unified messaging

mailbox. 1) When a caller leaves a voicemail message for the subscriber, the message is stored digitally on the computer(s) of the UC service provider. 2) The UC service provider then sends, via e-mail, a standard MIME encoded (or similar) document to the subscriber which contains at least one part. The first part is a standard HTML, WML or XML formatted document which contains interaction controls (e.g., URL links or form elements) linked backed to at least one server side program. When one of the interaction controls is selected, a message is sent back to the server causing the server to perform a corresponding one of the communication services. As described above, the MIME-encoded e-mail message also can contain, if the user prefers, the actual multimedia portion of the message attached as a separate MIME part to the e-mail so that the subscriber can listen to or view the message off-line (i.e., without a network connection). 3) Once the recipient receives the e-mail message and opens it, the recipient sees the graphical HTML, WML or XML attachment either directly in an e-mail client or in a Web Browser depending on the system configuration. Moreover, once the e-mail is opened, a communications connection (e.g., a Hyper Text Transfer Protocol (HTTP) connection) is established to an information server (e.g., a Web Server) which immediately loads images, data, or programs (like a Java applet or similar) necessary to construct the interface to be displayed. This interface may even provide current up-to-date information which is newer than the time and date the e-mail was originally constructed. The message identification (as well as other system parameters needed to retrieve the message) is also contained in the MIME message. 4) After opening the e-mail message, the subscriber is presented with a graphical user interface which can (1) retrieve the subscriber's message and (2) coordinate other communication services. The interaction controls also can load information dynamically and automatically into the document once the e-mail is opened (i.e., without requiring explicit user action after opening the e-mail). 5) Once the subscriber is finished with the message, the subscriber may delete the message like any other e-mail message. However, if the subscriber chooses to keep the message in the e-mail client, the subscriber will still be able to see up-to-date information (e.g., like the status of an account) when the message is opened again. This occurs because all time sensitive information is loaded dynamically each time the e-mail message is opened.

Detailed Description Text (43):
The interface allows the user to setup and configure a corresponding enhanced services account., including routing schedules for voice, fax, e-mail, and video calls and messages. The setup and configuration options that are available depend on the enhanced services to which the user subscribes. The enhanced services include, but are not limited, to: voice, fax, video mail find me/follow me services call diversion call screening text-to-speech conversion automatic speech recognition conferencing broadcast fax and voice messaging unified messaging and communications calling card

Detailed Description Text (58):
When the Unified Communications System sends a notification to an e-mail system with a copy of a non-literal message or a link attached, a synchronization problem is created. This occurs because a copy of or a reference to the message exists in two places. Automatic synchronization between the two systems eliminates the need for the subscriber to delete the message from two locations when it is no longer needed. This method allows a Unified Messaging view of (1) e-mail and (2) voice and FAX messages even if they do not share the same storage devices or locations. Accordingly, various Unified Communications and e-mail systems can be coupled together without storing all messages in a single location.

Version 8.0 of pcAnywhere remote control software gets rolled out

Network World; Framingham; Aug 18, 1997; Tim Greene;

Duns: **06-469-6941**
Volume: 14
Issue: 33
Start Page: 15
ISSN: 08877661
Subject Terms: Product introduction
Remote control
Software
Classification Codes: **9190**: *US*
5240: *Software & systems*
9120: *Product specific treatment*
9000: *Short article*
Geographic Names: US
Companies: Symantec Corp *Ticker:* **SYMC** *Duns:* **06-469-6941**

Abstract:
In August 1997, Symantec Corp. introduced a Windows NT-friendly update to its pcAnywhere32 software, a program that gives end users remote control of their PCs. With pcAnywhere32 8.0, companies can use Windows NT authentication software to define end-user access to networked PCs. Traffic also can be encrypted using Microsoft Corp.'s Crypto API.

Full Text:

Cupertino, Calif.

Symantec Corp. last week introduced a Windows NT-friendly update to its pcAny-- where32 software, a program that gives end users remote control of their PCs.

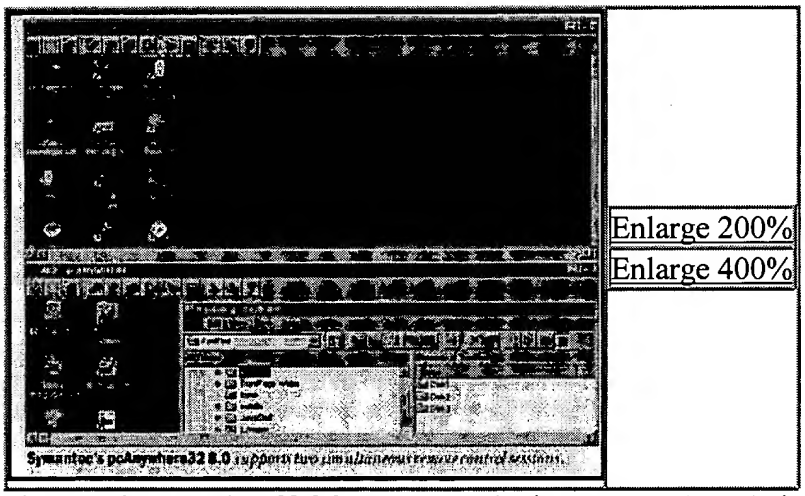
With pcAnywhere32 8.0, companies can use Windows NT authentication software to define end-user access to networked PCs. Traffic also can be encrypted using Microsoft Corp.'s Crypto API.

In addition, pcAnywhere32 logs can be recorded in a Windows NT event log for review by net administrators. Using a new utility, administrators also can stop, start and check the status of Windows NT **PCs** being accessed via dial-up lines. Version 8.0 also lets **remote** users print files accessed on an NT **PC**. In addition to Windows NT clients, the new Symantec software supports Windows 95, 3.1 and DOS clients. Aside from the new NT-related features, Version 8.0 supports switching between a **remote** control session and a voice call for **remote** users dialing in with standard data/fax modems. The software also can handle simultaneous voice and data sessions.

Another feature allows end users to lock a **PC** when the **remote** connection is broken, preventing anyone physically near the desktop **computer** from **accessing** it.

Multiple remote end users can log on to a single PC using pcAnywhere32 8.0, enabling remote training sessions and other applications.

Version 8.0 is available now and costs $149 for two licenses. Current customers can upgrade for $79. Symantec: (800) 441-7234



Symantec's pcAnywhere32 8.0 support two simultaneous remote control sessions.

Remote Access Networking: Riding the Wave of Portability

InfoWorld; San Mateo; Oct 5, 1992; Maxwell, Kimberly;

*Duns:*03-778-7298 *Duns:*08-146-6849 *Duns:*10-828-0991

Volume: 14
Issue: 40
Start Page: 58
ISSN: 01996649
Subject Terms: Solutions
Software packages
Remote control
Manyproducts
Manycompanies
Local area networks
Data transmission
Applications
Corporate purchasing
Computer networks
Classification Codes: **9190**: *US*
5250: *Telecommunications systems*
5240: *Software & systems*
Geographic Names: US
Companies: Novell Inc *Ticker:*NOVL *Duns:*03-778-7298
Microsoft Corp *Ticker:*MSFT *Duns:*08-146-6849
Datastorm Technologies Inc
Da Vinci Systems Corp
Banyan Systems Inc *Duns:*10-828-0991

Abstract:
*The solution to the frustration of **accessing** local area networks (LAN) from a **remote** location is usually a combination of hardware and software tools. Electronic mail is one of the most widely used **remote** applications, with a broad range of solutions. Programs such as Da Vinci Systems' Da Vinci eMail **Remote** can exchange messages with commercial services. Data transfers are generally the next step up from e-mail, and these can be achieved through transfer utilities that allow a user to dial up a modem-equipped **PC** attached to the network or that use asynchronous communications software. A **remote** control program can be an effective way to get into the network if it is necessary to access more than one application from afar. **Remote** control programs allow a distant **computer** to take over a machine attached to the network. **Remote** control systems also have their drawbacks. **Remote** nodes are the top of **remote** access, providing total*

*access to a LAN from a **remote** or mobile **PC**. Security should be a consideration for network administrators.*

Full Text:

While just about everyone travels with a notebook computer these days, plugging into corporate LAN resources continues to frustrate many users. Ideally, most users would like to plug their portables into standard phone jacks, dial a number, and receive the same access rights and drive mappings they have when they're in the office. That's possible, but it's not always the best choice. Many simple applications, such as electronic mail, can be well served with simpler and less costly solutions.

LAN Manager and Vines users already have this capability and can activate it by purchasing software utilities. NetWare users aren't so lucky; Novell's architecture requires additional (and expensive) hardware.

No matter what the network OS, the right solution is usually a combination of hardware and software tools and the recognition that some tasks are best left in the office or must be significantly reconfigured for remote use. The good news is that a wide range of tools and utilities are now available that facilitate remote LAN usage, and network vendors have begun to recognize the importance of this kind of access.

With the capabilities and performance of remote access products improving rapidly, it makes sense to buy just the solution that's needed now and not try to predict the future. If remote users only need E-mail, for example, don't buy a system that provides full access to network directories and resources. Fortunately, remote access tasks are pretty easy to pin down.

E-MAIL. E-mail is one of the most widely used remote applications, with a broad range of remote access solutions. Many packages have a feature that lets remote users dial up a centralized mail hub attached to the network so users can exchange messages. A mail server with one or more phone lines is attached to the network, and a custom version of the software is installed on portables.

Alternatively, public E-mail services can be used via a gateway with the corporate E-mail system. Although it's a bit more clumsy, this is often a faster and (in the short term) lower cost solution. E-mail programs such as cc:Mail and DaVinci can exchange messages with commercial services including MCI, CompuServe, and even the Internet.

Although this type of access is easiest to establish, there are some problems. First, high-volume users, especially those sending large files, will quickly find themselves with extravagant E-mail bills. Second, while many E-mail programs are quite adept at retrieving messages from the commercial services, sending messages often requires a lengthy and arcane address. Finally, services such as MCI and CompuServe, while reasonably secure, are not private and can be a security risk.

MOVING FILES. Data transfers are generally the next step up from E-mail. If the files are few or their size is small, it generally makes sense to use the file transfer capabilities of your E-mail package. If you don't have an E-mail solution or find that it doesn't meet your needs, there are several other options. Some of these solutions are as simple as file transfer utilities that let you dial up a modem-equipped PC attached to your network. LapLink Pro, for example, provides easy access to the hard disk of another computer as well as any network drives that computer is attached to. But you must run the program before you hit the road or have someone in your office do it for you; LapLink provides no log-in facilities.

You can also use asynchronous communications software (such as DataStorm's ProComm or Digital Communications Associates' Crosstalk), again exchanging files with a computer logged onto the company or department network. Although these programs offer highly efficient file transport protocols that save time and money, they can be complicated, and nontechnical users may resist them.

REMOTE CONTROL. When users need to access more than one application from afar, a remote control program like Norton-Lambert's Close-Up or Triton Technologies' CO/Session can be a quick and cost-effective way to get into the network while on the road. Remote control programs are utilities that let a distant computer "take over" a machine attached to the network. The remote computer functions as the keyboard and screen while all the processing remains on the local system. This is often a low-cost solution, because the software is typically just $100 to $200 per node and existing machines and modems are used at the LAN end.

Despite their attractive pricing, remote control programs have several drawbacks. First, only one user may dial into each local system at a time, and this system must be set up and turned on before the user leaves the office.

Second is the security risk; most users will prefer to use their own desktop system as the gateway, and leaving an unattended system logged onto a network is never a wise idea. Finally, performance can lag, especially with graphics or Windows applications, and programs that use unusual graphics modes or keyboard drivers will not work.

NetWare users can choose Novell's NetWare Access Server, a more sophisticated remote control offering that creates as many as 16 virtual machines on a single 386-or 486-based PC, each of which can be used by a remote computer. Although Novell's solution is expensive ($2,395 for the software, plus the cost of a high-powered PC and additional modems), it solves many of the logistical problems associated with remote control software.

Although remote control is not an ideal solution, it continues to serve many users well, especially as other remote access technologies continue to evolve. Capital Cities/ABC, the New York-based publishing and entertainment firm, uses Symantec's PC Anywhere to supplement its remote access capabilities, as the program supports leased telephone lines, a feature lacking in the remote access servers it also uses.

REMOTE NODES. For the ultimate in remote access, a better answer is in order: the creation of remote nodes. A remote node duplicates the local node at the user's desk, so it provides total access to your LAN from a remote or mobile PC. All security. mappings, and access privileges are maintained for each user--a completely invisible connection.

From any place with a phone line, you can map drives and printers, exchange files and E-mail, and even run network applications. Of course, because all this occurs over dial-up lines, response time may lag, especially with graphics and Windows-based applications. It can also be expensive, especially if you are supporting a large number of remote users on a NetWare network. But this approach can reduce training and support costs since drive mappings and application paths can be identical to those back in the office.

Remote nodes can be created through a server software utility on LAN Manager and Vines networks. Microsoft and Banyan sell $995 and $1,495 utilities, respectively, that install on a server and create nodes for users dialing in through a modem.

NetWare installations require an intelligent communications device connected between the LAN and dial-up lines. These devices, often called remote access servers, can be as complex as routers, offering flexible connectivity with a wide range of portable computing platforms and telecommunications standards. For example, Centrum Communications' Centrum Remote can give simultaneous access to as many as 16 users through both dial-up and T1 lines.

Most remote access servers lead dual lives; Shiva Corp.'s NetModem, for example, lets multiple users on the network dial out via one phone line to remote hosts, information services, or another network in a different location.

NetModem is perhaps the best-known remote access server. It duplicates a network node across telephone lines, making the remote user a part of the local network. Capital Cities uses NetModems so freelance writers can access the media giant's LANs to submit stories and work on drafts with editors. The MIS people also like the NetModem because it allows them to perform network management functions when they're not in the office. "I'm able to administer the network from a remote location," says Joe Kaiola, MIS communications director. "This keeps us from having to hire an MIS person at the site to maintain the network."

TAKING IT ON THE ROAD. No matter which product you choose, it's likely to take some time setting it up and some tweaking until it's working just right. Part of the equation is figuring out just what is and is not a practical application for remote computing. Even with efficient modems and data compression, there are some tasks that just don't travel well and others that may need to be rethought to make best use of portable resources.

One user site that discovered this fact was Turner Construction, a New York contracting concern with 35 offices located across the country. Turner uses Vines and bought Banyan's PC Dial-In remote access server to give mobile users access. Each office has one file server set up with Dial-In to allow the offices to communicate with each other and with company representatives in the field.

"We primarily use Dial-In for dialing back to the controlling offices and passing data and mail," explains John Good, Turner's director of information technology. Much of the data sent is E-mail, schedules, project data, and spreadsheet information, Good says.

Turner found Dial-In to be a very effective tool for communications between remote users at project sites and

offices but didn't use it to actually load network applications on remote PCs. "We didn't design our implementation of Dial-In to load network applications remotely," Good says.

Other businesses are discovering that remote access can give them a competitive edge. Canaan Analytics of New Castle, Del., is a company specializing in client/server computing that has several money management firms as clients. "Stockbrokers need to keep track of portfolio holdings and track market quotes, and they can't keep all of this information on their laptop. They must have a way to access the network effectively," says John Tarbox, Canaan's owner and president. "Many people feel like they are cut off from the network when they are away from the office. With (the right) solution, your portable is like being at your desk."

Tarbox says his clients primarily use LAN Manager's Remote Access Service, a software add-on priced at $995 per server, to dial up their LAN Manager networks 24 hours a day. He adds that he also can dial up the network, having supervisory rights, and as long as nothing "catastrophic" occurs, such as file servers going down, he can troubleshoot network problems.

Like Vines Dial-In, Remote Access Service uses the security configuration found in the file server, and you don't have to set up a special server to provide these services to the remote user. You can use the main file server, equipped with standard modems, as the link for remote access.

SECURITY AND ACCESS. Before anyone gets remote access, network administrators must consider security. Obviously, any time, additional points of access are added, the risks of unauthorized use increase. Letting someone dial in to a network can be a touchy subject for some network administrators. Some believe remote and mobile users are uncontrollable and may run wild over the network. However, those concerns are usually short-lived once the administrator sees they can have pretty much the same or more control over remote users accessing the network and its resources. Depending on the solution, the user will have specific user rights to the network resources attached to their user ID and password, just as they do when they are directly connected. Some of the remote solutions are so tightly integrated into the network's security system that there isn't any special configuring done for remote users who log on to the network.

All of the solutions discussed here have one thing in common--they all use dial-up phone lines to connect the remote machine and the network. For most companies, standard asynchronous telephone lines are the most cost-effective way to communicate. However, heavy usage or regular traffic between two sites may make other services, such as leased lines and packet-switched networks, more attractive. Although it takes more effort to set up this kind of connection, the ultimate cost of service can be much lower.

REMOTE FUTURE. Today we are working away from the office more often, so it's necessary to find solutions that free us from the office. If you depend on a computer network for much of your work, there's no reason you should feel like you have to be in the office to access or use the files or applications on the office's network. With special hardware and software products and existing telephone lines, your remote PC can access the company network no matter where the road takes you.

Kimberly Maxwell is a Florida-based freelance writer specializing in networks and connectivity.

AMERICAN SYSTEMS: PC Remote makes it easy to access other computers

M2 Presswire; Coventry; Jun 8, 1999;

Start Page: 1

Abstract:
M2 PRESSWIRE-8 June 1999-AMERICAN SYSTEMS: PC Remote makes it easy to access other computers (C)1994-99 M2 COMMUNICATIONS LTD

PC Remote allows end-users to determine who can access their computer and whether or not that person can transfer files back and forth. The system is totally secure, with each user being assigned a username and password. Connection "profiles" can be created so frequently used connections can be established with just a few mouse clicks. The host portion can be automatically loaded when Windows starts, making it easy to access a work computer from home, or a home computer while away on business. One can clearly see everything on the other screen and have full control of the keyboard and mouse.

Full Text:

M2 PRESSWIRE-8 June 1999-AMERICAN SYSTEMS: PC Remote makes it easy to access other computers (C)1994-99 M2 COMMUNICATIONS LTD

Fort Worth, TX -- American Systems announces the release of **PC Remote** 1.0, a program for **accessing remote computers** in a variety of ways. Connections can be made across a LAN, over a modem, using the **computer** serial ports, and across the Internet.

PC Remote allows end-users to determine who can access their computer and whether or not that person can transfer files back and forth. The system is totally secure, with each user being assigned a username and password. Connection "profiles" can be created so frequently used connections can be established with just a few mouse clicks. The host portion can be automatically loaded when Windows starts, making it easy to access a work computer from home, or a home computer while away on business. One can clearly see everything on the other screen and have full control of the keyboard and mouse.

"With PC Remote," said American Systems President Matt Porter, "we wanted to give people a way to access other computers in a fast, efficient, and inexpensive way. With more and more people dealing with multiple computers, at home and at work, getting easy access to data and files can be a real problem. PC Remote provides a viable solution."

PC Remote provides complete keyboard and mouse control of the remote computer, as well as macros that can be executed just as if they were being run on the remote machine. Data can be copied to the clipboard on the remote compute and instantly appear in the clipboard of the controlling computer. The end-user can select between image quality and speed, making the product extremely flexible. The data flow can also be paused, while doing other tasks, and then resumed when desired.

The intuitive interface makes PC Remote the perfect tool for both new and experienced users. Unlike other programs that are extremely complex, PC Remote is easy to understand and use. On a LAN, it can automatically scan to find other machines running the program and on a modem connection it quickly determines what serial port is being used for making the call.

System requirements

PC Remote will run under Windows 95/98 and NT 4.0. It requires 2 megabytes of disk space and 8 MB of RAM.

Price and Availability

PC Remote will be available June 3, 1999 from the American Systems home page at http://www.americansys.com. The price is $49.95.

American Systems, based in Fort Worth, Texas, develops personal productivity and utility products, which enhance and simplify the operation of the Windows platform. Well-known titles from the company include Print Screen Deluxe, EZ Macros, EZ Scheduler, Tidy Disk, Print Screen, and Internet EZ Search.

M2 COMMUNICATIONS DISCLAIMS ALL LIABILITY FOR INFORMATION PROVIDED WITHIN M2 PRESSWIRE. DATA SUPPLIED BY NAMED PARTY/PARTIES.

PCWORLD.COM
TECHNOLOGY ADVICE YOU CAN TRUST

PCAnywhere Turns 11

Symantec's remote-access app offers updated look, easier file transfers.

Matt Hamblen, Computerworld
Monday, June 02, 2003

Monday, Symantec plans to announce PCAnywhere 11, an upgraded release of its remote-access software that features performance improvements and a revised user interface for IT help desk administrators.

The PCAnywhere technology, which was initially released in 1986 as a connectivity tool for remote users, has emerged in recent years as a help desk support tool. The software provides help desk workers with remote system control functions, including the ability to take over a PC in the field and transfer files or patches, said David Scott, a senior product manager at Symantec in Cupertino, California.

The new version can transfer needed files in the background while IT administrators continue with other work, Scott said. He added that the revamped user interface looks more like Windows XP and offers increased configuration flexibility, making it possible to reduce the size and number of tool bars and other features.

To the Test

The Burlington Northern and Santa Fe Railway in Fort Worth, Texas, has about 250 PCAnywhere users and is beta-testing the version 11 release, said Brian Cook, a field service engineer at Wabtec. Cook works at BNSF under an IT services contract between the railway company and Wilmerding, Pennsylvania-based Wabtec. The upgraded software provides faster remote connections and better response-time performance than existing versions of PCAnywhere, and it has a better look and feel, he said.

One big benefit of using PCAnywhere is that it lets help desk staffers take control of PCs so they can show users how proprietary BNSF applications work, Cook said. And if a user's system won't start, PCAnywhere can be used to access a fail-over copy of the user's data at a backup site in Topeka, Kansas, and restore the PC.

"I have no qualms with this product," Cook said. "If they raised the price, people would still buy it."

In Control

Framingham, Massachusetts-based IDC recently reported that PCAnywhere commands more than 50 percent of the global market for remote systems control software, outpacing products from Symantec's four major competitors: Tivoli Software, Computer Associates International, LANDesk Software, and Danware Data A/S.

"The remote-control market is very mature, so products are at a very high level of functionality," said IDC analyst Stephen Drake.

Products like PCAnywhere also face competition from the free remote-control capabilities that Microsoft has built into Windows XP, Drake added. The market for remote-control software will stay about level with last year's sales of $288 million for several more years, he predicted.